Topi Hellsten

IoT-PROTOKOLLAT

Tietojenkäsittelyn koulutusohjelma

2014

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

IoT-PROTOKOLLAT

Hellsten, Topi
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
marraskuu 2014
Ohjaaja: Grönholm, Jukka
Sivumäärä: 44

Asiasanat: iot, ioe, iot-protokollat

Tämän opinnäytetyön tarkoituksena on tutustua uuteen teknologiseen trendiin nimeltään Internet of Things. Mikä se on, miksi ja miten.

Opinnäytetyön alussa aihetta käydään läpi yleisellä tasolla. Tutkin tarkemmin aiheen käsitteistöä, kehitysvaiheita, merkitystä liiketoiminnalle sekä turvallisuutta. Kerron myös esimerkkejä siitä, mikä tarkalleen ottaen on IoT (Internet of Things) ja miten se näkyy tavalliselle kuluttajalle arkielämässä.

Opinnäytetyön päätavoitteena on perehtyä tarkemmin IoT-protokolliin. Tavoitteena ei ole opiskella kaikkia protokolliin liittyviä yksityiskohtia, vaan enemmänkin saada niistä yleiskäsitys ja tieto siitä, mitä on saatavilla. Käsittelen aluksi yleisellä tasolla mitä tarkoittaa termi protokolla, ja mihin sitä tarvitaan. On olemassa erityisiä protokollia, joita yleisesti käytetään IoT:hen liittyviin sovellutuksiin. Protokollat, joita työssäni käyn läpi, ovat: MQTT, CoAP, XMPP, AMQP, Z-Wave, ZigBee, DDS, ja INSTEON.

Osallistuin myös kesällä aiheeseen liittyvään käytännön projektiin kouluni kautta. Olin seitsemän viikkoa palkallisessa harjoittelussa, jossa tavoitteena oli aikaansaada toimiva aiheeseen liittyvä kokonaisuus. Kerron opinnäytetyössäni projektista niin yleisesti, kuin myös tarkemmin siitä, mitä sillä lopulta saavutettiin. Esittelen tehtyä sovellusta järjestelmätasolla ja pintapuolisesti, menemättä sen tarkemmin sovelluksen ohjelmointiin. Esittelen myös laitteistoa, jota projektissa käytettiin. Lopuksi pohdin projektin merkitystä niin itselleni, kuin myös muille.

IoT-PROTOCOLS

Hellsten, Topi
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in data processing
November 2014
Supervisor: Grönholm, Jukka
Number of pages: 44

Keywords: iot, ioe, iot-protocols

The purpose of this thesis is to get to know the new technological trend called the Internet of Things. What it is, why and how.

At the beginning of the thesis the subject is reviewed at a general level. I look closer into the subject's concepts, developmental phases, significance to business, and security. I also mention examples of what the IoT (Internet of Things) really is and how it can show up on a regular consumer's everyday life.

The main goal of the thesis is to take a closer look into the IoT-protocols. The priority is not to learn every detail there is to know about the protocols, but on the contrary to get an overview of them and knowledge of what there is available. At first on a general level I deal with what does the term protocol mean and what's it needed for. There are specific protocols, which are commonly used for IoT –related applications. Protocols, which I go through in my thesis, are: MQTT, CoAP, XMPP, AMQP, Z-Wave, ZigBee, DDS, and INSTEON.

During the summer I also participated in a hands-on project related to the subject through my school. For seven weeks I was in a paid apprenticeship, where the objective was to accomplish a working entity related to the subject. In my thesis I talk about the project in general, and also more of that, which was eventually achieved with it. I demonstrate the program made superficially and on an architectural level, without going into detail of the programming behind it. I also present the hardware used in the project. Finally I ponder the meaning of the project to myself, as well as to others.

SISÄLLYS

1 JOHDANTO

Kaikki puhuvat Internet of Things:istä. Se lupaa olla yksi suurimmista teknologisista vallankumouksista mitä ihmiskunta on ikinä nähnyt. Silti monetkaan ihmiset eivät ymmärrä, että standardit ovat IoT:n perusta. Ilman niitä, tätä vallankumousta ei voi tapahtua. Internet itsessään toimii standardien pohjalta, ja juurikin standardit mahdollistavat toisilleen ja ihmisten kanssa kommunikoivat esineet.

IoT on kehittyvä ilmiö, joten on olemassa monia eri tapoja tarkastella sitä. Usein se jaetaan osiin, jotta sitä olisi helpompi ymmärtää. Eri osat yhdistyvät & ovat vuorovaikutuksessa toisiinsa ja muodostavat kaikenkattavan käsitteen Internet of Things. IoT voidaan jakaa neljään helposti ymmärrettävään osaan: puettavat laitteet, äly- kodit ja kodinkoneet, toisiinsa yhdistetyt ajoneuvot, ja älykkäät kaupungit.

Olemassa olevia standardeja käytetään jo jokaisella edellä mainitulla osa-alueella, ja uusia standardeja kehitetään parhaimmillaan täyttämään aukkoja. Kun IoT realisoituu sen mahdollistavien standardien myötä, syntyy valtaisia markkinamahdollisuuksia uusille yrittäjille. Edelleen jotkut väittelevät siitä, miten IoT:n kehittymiseen menee vielä kymmenestä viiteentoista vuoteen aikaa. Muut ovat sitä mieltä, että IoT on jo täällä. Siitä ei tule todellisuutta yhtäkkisesti. Sen sijaan, se tunkeutuu päivä päivältä arkiseen elämäämme.

Puettavat laitteet ovat mahdollisesti näkyvin todiste tulevasta Internet of Things:istä. Älykellot, sykemittarit, Google Glass – älylasit, diabetesmittarit, ja fitness - rannekkeet ovat vain muutamia esimerkkejä vekottimista, joita ihmiset alkavat kantaa mukanaan. Ja tietysti älypuhelimet, jotka yhdistyvät näihin laitteisiin, ovat myös osa IoT:tä.

Puettavissa laitteissa on tehty mielenkiintoinen erotus toisistaan: ne, jotka liittyvät lääkäreihin ja sairaaloihin, ja ne, jotka eivät. Laitteet, jotka liittyvät lääketieteeseen, mielletään lääketieteellisiksi ja kirurgisiksi kojeiksi. Sellaisenaan ne vaativat hyväksynnän FDA:lta (Federal Food and Drug Administration) ennen kuin niitä voidaan

laittaa myyntiin. Tämän takia, tästä osasta Internet of Things:siä ei tule vielä useaan vuoteen arkipäivää.

Älykodit ja älykkäät kodinkoneet tekevät tuloaan. Turvajärjestelmät ja termostaatit tulevat entistä enemmän tietoiseksi kodeissaan asuvista ihmisistä, tarkkaillen ja reagoiden heidän käytökseensä. Älykäs jääkaappi voi esimerkiksi kertoa, että ovi on jäänyt auki ja ruuat sulavat. Älykodit voivat jopa pelastaa ihmishenkiä vanhainkodeissa tarkkailemalla asukkaiden sijaintia ja elonmerkkejä.

Toisiinsa yhdistyvät ajoneuvot, kuten itsestään ajavat autot, tulevat suuresti muuttamaan ihmisten tapaa liikkua paikasta toiseen. Jo tälläkin hetkellä useat uudet autot pystyvät kommunikoimaan omistajiensa kanssa RFID:n (Radio Frequency Identification) kautta välittäen tietoa tietokoneisiin ja älypuhelimiin. Kun auton rengaspaineet laskevat liian alas, omistajaa informoidaan tästä tekstiviestillä tai sähköpostilla. On myös jo olemassa autoja, joista on täysi pääsy Internetiin, ja jotka pystyvät parkkeeraamaan itse itsensä. Useimmat kuluttajat tulevat omaksumaan IoT:n osaksi niin henkilöautojaan, kuin kodinkoneitaan siinä vaiheessa, kun on aika hankkia uusi vanhan tilalle. Autonvalmistajat esittelevät erikseen ostettavia lisävarusteluja, joilla autoon voidaan tuoda IoT:n teknologiaa, joten toisiinsa yhdistyvien ajoneuvojen kokonaismäärä voi kasvaa dramaattisesti jo muutaman vuoden aikana.

Älykkäillä kaupungeilla tulee olemaan valtavia määriä IoT - teknologiaa käyttäviä sovellutuksia. Yhdistyneet kansakunnat (YK) ennustaa, että vuoteen 2050 mennessä kaksi kolmasosaa maailman väestöstä tulee asumaan kaupungeissa. Ruuhkat, energiatarve, ja huoli terveydestä ja turvallisuudesta ovat kaikki tulevia käyttökohteita. Älykkäässä kaupungissa autoilijat ohjataan tyhjiin parkkiruutuihin. Energian tuottoa ja kulutusta säännellään ja ohjataan sinne, missä sitä hetkellisesti eniten tarvitaan. Älykkäät lääketieteelliset kojeet minimoisivat turhat sairaalakäynnit ja hälyttäisivät apua vain silloin, kun sitä todella tarvitaan.

Älykkäät kaupungit kuulostavat futuristisilta, mutta parasta aikaa hallitukset miettivät mitä IoT voisi tuoda lisää kaupunkiensa asukkaille. Jokaisen älykkään kaupungin ytimessä ovat standardit ja Internet, joka tietysti itsekin on rakennettu standardien pohjalta. (Bartleson, haettu 22.11.2014.)

2 INTERNET OF THINGS

2.1 Käsitteet

Internet of Things ei ole teknologisesta näkökulmasta katsottuna varsinaisesti uusi asia. Siitä on puhuttu erilaisin termein jo toistakymmentä vuotta. Ajan kuluessa on syntynyt uusia käsitteitä, joilla myös osaltaan tarkoitetaan hieman erilaisia asioita. Siksi usein tuleekin vastaan erilaisia käsitteitä esimerkiksi median kautta, ja tulee miettineeksi mistä milloinkin on kyse. Seuraavaksi käsittelen osan useimmin eteen tulevista käsitteistä.

Kronologisessa järjestyksessä käsitteet menevät seuraavalla tavalla: Pervasive Computing, Ubiquitous Computing (suom. jokapaikan tietotekniikka, läsnä-äly), Machine to Machine (M2M), Internet of Things (IoT), Internet of Everything (IoE), Industrial Internet. Käsitteistä Pervasive Computing ja ”Ubicomp” ovat melko vanhentuneita, joten jätän ne käsittelemättä tässä yhteydessä. (Stateham, haettu 22.11.2014.)

Käsitteellä Machine to Machine tarkoitetaan kahden erillisen laitteen välistä kommunikointia ja tiedonsiirtoa. Useimmiten tiedonsiirto tapahtuu sensoreiden, kuten lämpötila, sijainti, liike, korkeus, nopeus, jne. kautta. Laitteisiin liitetyt sensorit tallentavat tapahtumia, jotka ne välittävät tietoliikenneyhteyden välityksellä edelleen tarvittuun kohteeseen. Sensori voi esimerkiksi sisältää SIM-kortin, joka kykenee välittämään ja vastaanottamaan dataa. Tieto välitetään edelleen palvelimella sijaitsevalle sovellukselle, joka analysoi tiedon ja voi tehdä tarvittavia jatkotoimenpiteitä sen pohjalta. (Vodafone.)

Industrial Internet on kokonaisuus, jota kutsutaan myös teollisuuden neljänneksi vaiheeksi, on johtanut käsitteen Industrial Internet of Things – syntyyn. Siinä toisiinsa yhdistyy entistä monimutkaisempia laitteita, isoja koneita ja järjestelmiä älykkäiden sensorien avulla. Industrial IoT yhdistää enemmänkin isoja kokonaisuuksia toisiinsa, joten tavallinen kuluttaja ei tule tätä välttämättä edes huomanneeksi. Tavallisen kuluttajan IoT sisältää laitteita, kuten älypuhelin, televisio, jääkaappi, mikroaaltouuni jne., kun Industrial IoT yhdistää toisiinsa rekkoja, tuulimyllyjä, metroja, ja voimalai-

toksia. Esimerkiksi, raskaisiin rekkoihin upotettu teknologia voi optimoida reittejä, huomioiden matkojen pituudet ja polttoaineen kulutuksen. Laiterikon uhatessa esimerkiksi tuulimyllyissä, sensori voi hälyttää ajoissa insinöörin paikalle ennen vahingon tapahtumista. (Santori, haettu 22.11.2014.)

Käsitteistä Internet of Things (IoT) ja Internet of Everything (IoE) ovat kaksi käytetyintä. IoE on yrityksen nimeltä Cisco lanseeraama käsite. Heidän mukaansa tulisi tehdä selvä ero käsitteiden IoT ja IoE välille, mutta käytännössä ne tarkoittavat samaa asiaa. Ciscon mukaan IoE yhdistää toisiinsa ihmiset, prosessit (miten ihmiset, tieto, ja esineet toimivat yhteen), datan, ja esineet/asiat. Tavoitteena on tehdä verkottuminen tärkeämmäksi ja arvokkaammaksi, kuin koskaan ennen. Informaatio muunnetaan teoiksi, jotka luovat uusia kykyjä, rikkaampia kokemuksia ja ennennäkemättömiä taloudellisia mahdollisuuksia liiketoiminnalle, yksilöille, sekä valtioille. Tällä ajattelumallilla IoE koostuu siis neljästä eri osatekijästä: ihmiset, prosessit, data, ja esineet. Internet of Things nähdäänkin vain yhtenä osana, esineinä, jotka toimivat IoE:n taustalla. Internet of Everything vie edelleen eteenpäin Internetin voimaa parantaa liiketoiminnan ja teollisuuden lopputulemia, ja ennen kaikkea parantaa ihmisten elämiä tuomalla lisää Internet of Things:in edistykseen. (Evans, haettu 22.11.2014)

2.2 Käytännön sovellutukset

Internet of Things:issä erilaiset esineet ja laitteet verkottuvat toistensa kanssa sensoreiden avulla niin laitetasolla, kuin ohjelmallisestikin. Johdannossa käsitelty esineiden jaottelu suurempiin kokonaisuuksiin ei kuvaa niitä yksilötasolla erityisemmin. Yksittäisissä tapauksissa erilaiset esineet ja niiden toimintaperiaatteet vaihtelevat toisistaan suuresti, ja venyttävät mielikuvituksen rajoja. Esineet keskustelevat toistensa kanssa ja vaihtavat tietoja:

- Älykellot, palohälyttimet ja parkkiruudut keskustelevat pian keskenään.
- Potilaan tahdistin hälyttää ilmoituksella mahdollisesta ongelmasta terveydessä lääkärille ennen, kuin tilanne muuttuu vaaralliseksi.
- Myyntiautomaatit kertovat itse, koska niitä tulee täyttää uudelleen.
- Autoteihin asennetut sensorit pystyvät kontrolloimaan liikenteen sujuvuutta.

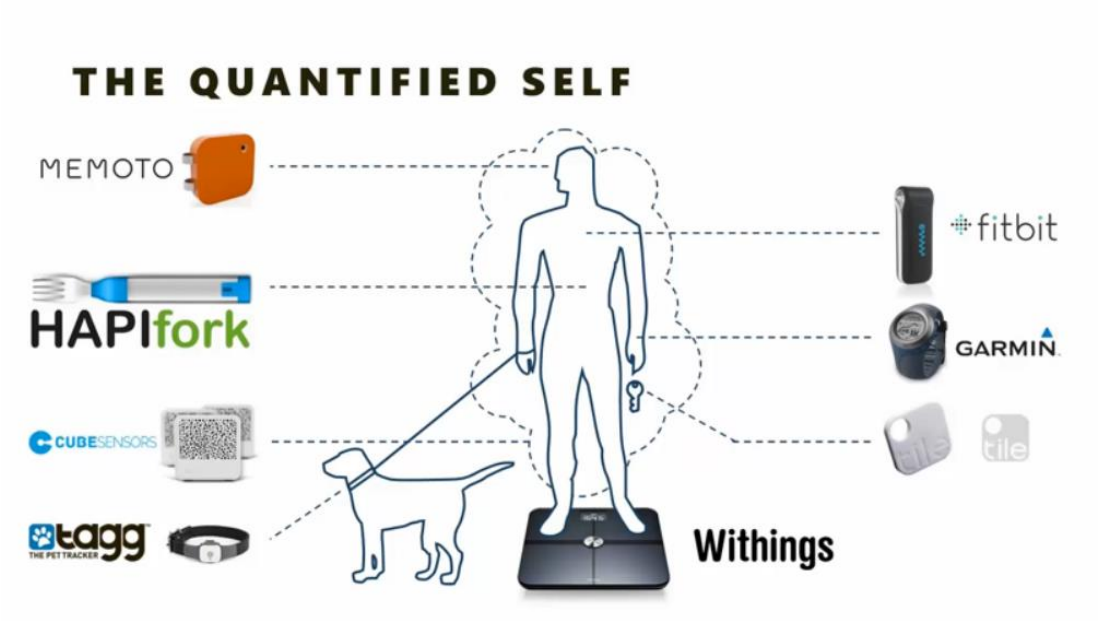
Internet of Things viittaa myös laitteisiin, joiden emme perinteisesti olettaisi olevan älykkäitä tai toisiinsa yhteydessä. Laitteet ovatkin usein hyvin arkisia, joilla on oma IP-osoitteensa. Oli kyseessä sitten pöytälamppu tai herätyskello, se voi olla älykäs.

GlowCap on yksi parhaista IoT-laite – esimerkeistä, joista on konkreettista hyötyä käyttäjänsä päivittäiseen elämään. GlowCap on älykäs lääkerasia, joka helpottaa varsinkin vanhemman väestön päivittäisen lääkeannoksen annostelua. Rasia muistuttaa valo- ja äänimerkein siitä, koska lääke tulisi ottaa. Lääkerasian kansi hohtaa oranssia valoa ja lähettää muistutuksia käyttäjälleen ja tarvittaessa myös käyttäjän lähiomaisille. Muistutus on mahdollista saada tekstiviestillä, kuin myös puhelinsoitolla. Rasian mukana tulee myös erillinen pistorasiaan kytkettävä erillinen huomiovalo, joka myös osaltaan muistuttaa käyttäjäänsä. Rasian kannen alaosassa on painike, josta painettaessa käyttäjän lähiapteekkiin lähtee tieto, että lääkkeet ovat vähissä. Tieto lähtee eteenpäin apteekkiin mobiilidatalla. Uusi annos lääkkeitä on valmiina noudettavaksi etukäteen määritellystä apteekista.
(GlowCap.)

Quantified self on ”liike”, jossa pyritään tuomaan henkilön jokapäiväiseen elämään mukaan mahdollisimman paljon teknologiaa. Henkilön toimintaa seurataan niin päivittäisellä, kuin pidemmälläkin aikavälillä. Esimerkiksi seurataan syömistä, ympäröivää ilmanlaatua, mielialoja, ja toimintakykyä (fyysinen & henkinen). Internet of Things liittyy kyseiseen liikkeeseen siinä käytettävien laitteiden ja esineiden osalta. Suosituimpia laitteita ovat esimerkiksi:

- FitBit, langaton aktiivisuusranneke
- Withings, henkilövaaka Internet-yhteydellä
- Memoto, langaton automaattikamera
- HAPIfork, syömisen vauhdin mittaava haarukka
- CubeSensors, ympäröivää ilmaa analysoiva sensori
- Tile, GPS-paikannin irtaimistolle
- Tagg, GPS-paikannin lemmikeille

(Stateham, haettu 22.11.2014.)



Kuva 1: The Quantified Self

2.3 Kehitysvaiheet

Vuonna 1999 Kevin Ashton esitteli ensimmäistä kertaa käsitteen the Internet of Things. Käsitteellä tarkoitettiin tunnistettavia esineitä, jotka esitettiin liittyvän toisiinsa Internetin kaltaisella rakenteella. The Internet of Things tunnettiin aikaisemmin nimellä ”control networks”. Reza Raji kuvaili konseptia seuraavasti: ”Pieniä datapaketteja liikkuu suurelle määrälle ”solmuja”, jotta voitaisiin integroida ja automatisoida kaikki kodinkoneista, aina suuriin tehtaisiin asti.” Raji loi vuonna 1998 varhaisimman IoT dokumentaation järjestelmästä, jossa pystyttiin kontrolloimaan ja monitoroimaan etäältä kotoa löytyviä laitteita. Tämän mahdollisti kamera, joka oli kytkettynä verkkosivustolle, jota käyttäjä pääsi hallitsemaan. (TechCrunch.)

Tällä hetkellä Internet of Things on jo vahvasti arkipäiväistynyt. Käsitteen alle mahtuu jo mielikuvituksen rajoja koettelevia laitteita, esineitä ja sovellutuksia, ja lisää on suunnitteilla koko ajan. Kilpailemaan ovat lähteneet niin pienet, kuin suuretkin yritykset, unohtamatta aivan yksilötasoa. Henkilöt, joilla on mielestään riittävän hyvä visio jostakin, voivat suhteellisen helposti kerätä varoja joukkorahoituksen (eng. crowdfunding, Kickstarter) keinoin, ja lähteä rakentamaan tuotettaan/yritystään.

Kansainvälisen tutkimus- ja konsultointiyritys Gartner:in mukaan IoT:n ”hypekäyrä” on jo saavuttanut huippunsa. Sen mukaan jokainen kasvava teknologia käy elinkaarensa aikana läpi luonnollisen prosessin, jossa teknologia saa syntynsä innovaatiosta ja lopulta saavuttaa liioiteltujen odotusten tason. Sen vanhetessa markkinat joutuvat ensin pettymään, ennen kuin siitä tulee osa jokapäiväistä elämää. (Butler, haettu 22.11.2014.)

Juuri tällä hetkellä 80 esinettä/asiaa yhdistää itseään Internetiin. Vuoteen 2020 mennessä kyseinen luku tulee olemaan 250, Cisco ennustaa. Toisiinsa yhdistyneiden laitteiden kokonaisluku tulee ennusteessa olemaan 50 miljardia. Kasvu on räjähdysmäistä. (Tillman, haettu 22.11.2014.)

Internet of Things:in evoluutiossa ei ole niinkään kyse uusista, vallankumouksellisista teknologioista, vaan enemmänkin uusista standardeista ja ohjelmistoista. Pohja, jonka päälle ryhdytään luomaan uutta, on jo valmiiksi rakennettuna. Eksponentiaalinen kasvu ei tule tapahtumaan ennen kuin IT-mallit ja protokollat ovat standardoituja. (Fahrion, haettu 22.11.2014.)

Uudet laitteet muuttuvat entistä pienemmiksi ja tietysti, älykkäämmiksi. Aina vain enemmän älykkyyttä leviää verkossa, jonka myötä vaaditaan vähemmän välitöntä ihmisen osallistumista. Laitteet tarvitsevat vähemmän energiaa ja ne osaavat käyttää sitä tehokkaammin hyödykseen. Internet of Things tulee olemaan enemmän kuin vain pieni älykkäistä laitteista koostuva verkottunut kokonaisuus. Se tulee sisältämään myös vanhaa laitteistoa, johon on jälkikäteen lisätty tarvittavat toiminnallisuudet ja älykkyys. (Fahrion, haettu 22.11.2014.)

Tulevaisuuden suurimmat haasteet tulevat IP-osoiteavaruudesta ja akkuteknologiasta. Jo tälläkin hetkellä viimeiset IPv4 (IP-osoitteiden nykyinen versio) – osoitteet ovat jaettu ja uhkaavat virallisesti loppua. Siirtyminen uuteen, IPv6 teknologiaan on varsinkin IoT:n kehittymisen myötä pakollista, ja se olisi tapahduttava mahdollisimman pian laajalti. Laitteiden akunkesto tulee olemaan osa suurempaa ongelmaa tulevaisuudessa. Esimerkiksi tämän hetkisten älypuhelinten akunkesto laahaa pahasti muuta teknologiaa perässä. Teknologiaa paremmin kestäviin akkuihin on olemassa joissain määrin, mutta se on aivan liian kallista käytettäväksi kuluttajatason laitteissa. Ener-

giatehokkuus, akkukapasiteetti ja virrankulutus ovat siis suuria haasteita. Kun IoT pyrkii yhdistämään kaikenlaisia laitteita toisiinsa, tulee pitää mielessä niiden toimintaperiaatteet. Ne vaihtavat tietoja IP-osoitteiden, jotka ovat loppumassa, mahdollistamana, ja ne toimivat akuilla, joiden akunkesto ei nykyisellä teknologialla ole varsinaisesti riittävä.

2.4 Merkitys liiketoiminnalle

Liiketoiminnan näkökulmasta, Internet of Things luo suurenmoisia mahdollisuuksia useille erityyppisille yrityksille. Yritykset voivat olla esimerkiksi IoT – sovelluksien tuottajia, palveluntarjoajia, IoT – alusta- ja integroinnin tarjoajia, telealan yrityksiä, sovellusten jälleenmyyjiä. Joidenkin arvioiden mukaan jo yksinään laitteiden välinen, ”machine to machine” – malliin perustuva liiketoiminta, tulee olemaan liikevaihdoltaan noin 714 miljardia euroa vuoteen 2020 mennessä. Lisäksi IoT:hen liittyvät pienemmätkin osasegmentit tulevat kasvamaan monikymmenkertaisiksi jo lähivuosien aikana. Näistä todennäköisimmin kasvavista osa-alueista mainittakoon kuluttajaelektroniikka, ajoneuvot, terveydenhuolto, sekä älykkäät rakennukset ja apuvälineet/työkalut.

Odotetunlainen, laaja IoT:n käyttöönotto edellyttää IoT:n liiketoiminnan ekosysteemien syntymistä. Jokaiseen ekosysteemiin kuuluu osa-aluetta edustavien yritysten ja yksityishenkilöiden yhteistyötoiminta. Jokaisen ekosysteemin sisällä yritykset kilpailevat keskenään, tehden myös tarvittaessa yhteistyötä. Yritykset pohtivat alueen tärkeimpiä tekijöitä ja voimavaroja, ja miettivät miten niitä voitaisiin soveltaa ja yhdistää fyysisestä maailmasta virtuaaliseen, Internetin maailmaan. Nämä tekijät voivat esiintyä laitteiston, ohjelmistojen, rajapintojen tai standardien muodoissa. Yksittäisille yrityksille, IoT:n nykytilannetta ja trendejä, voidaan kuvata teknologisten liiketoimintamallien keinoin.

Tällä hetkellä IoT - markkinat ovat hyvin varhaisessa vaiheessa, jossa on paljon sirpaloituneita, spesifisiä, vain tiettyyn tarkoitukseen luotuja ratkaisuja. Näihin kuuluu vielä yksityisomistuksessa olevia, patentoituja osasia, kuten sovellusalustat, protokollat, käyttöliittymät jne. Tällöin eri komponenttien tuottajien on lähes mahdotonta

tuottaa markkinoille mitään yleispätevää, jolloin yhteensopivuus kärsii ja hinnat pysyvät korkealla tasolla. Standardoituja, vapaaseen käyttöön tarkoitettuja protokollia ja rajapintoja vasta kehitetään, tai ollaan juuri vasta tuomassa markkinoille kaikkien saataville. Nämä seikat rajoittavat IoT:n kehitystä ja käyttöönottoa suhteettoman paljon. Oletettu, ripeänlainen IoT – markkinoiden kasvu, on paljolti riippuvainen yleisten, hallitsevien standardien ja rajapintojen esilletulosta.

Internet of Things:in liiketoiminnan ekosysteemit muodostetaan tiettyjen teknologisten ratkaisujen ympärille, keskittyen usein tiettyyn toimialueeseen. Toimialueita ovat esimerkiksi: RFID (radio frequency identification, radiotaajuinen etätunnistus), mobiilit laitteiden väliset AMR (automatic meter reading, automaattinen mittarinluenta) – yhteydet, tai ZigBee – protokolla älykodissa. Joidenkin arvioiden mukaan erilaisia IoT-palveluja tarjoavat yritykset tulevat saamaan suurimman osuuden IoT:hen liittyvistä rahallisista tuloista. Tällä hetkellä ekosysteemit hakevat vielä lopullista muotoansa tilanteessa, jossa niin virkaa tekevät yritykset, kuin uudet tulokkaat kilpailevat ja tekevät yhteistyötä samoilla markkinoilla.

Internet of Things – yritysten liiketoimintamallit vaihtelevat sen myötä, onko IoT ainoa myytävä palvelu/tuote, vai onko IoT vain jatketta jo olemassa olevalle myynnille. Vanhan yrityksen etu on siinä, että usein asiakaskunta on jo olemassa valmiiksi ja tehtäväksi jää vain vakuuttaa heille tuotteensa tarpeellisuus ja hyödyllisyys. Silti uskotaan, että uusien toimijoiden innovatiivisemmat liiketoimintamallit ja ideat tulevat muuttamaan ja edelleen muokkaamaan Internet of Things:iä, suuria toimijoita huomattavasti enemmän. (Mazhelis, Warma, ym., haettu 18.11.2014.)

2.5 Turvallisuus

Internetiin yhdistetyt älykkäät kodinkoneet lupaavat tekevänsä käyttäjänsä elämästä helpompaa. Mutta mikäli on uskominen Hewlett-Packardin tekemään tutkimukseen, suosituimmat älylaitteet ovat lähes yhtä turvallisia, kuin lukitsematon väliovi. Tutkijat tarkastelivat lähemmin kymmentä suosituinta, Internet-yhteydellä varustettua esinettä tai laitetta. Löydökset olivat järkyttäviä. Tutkituilla kymmenellä laitteella oli yhteensä laskettuna 250 erilaista aukkoa turvallisuudessa, joita hakkerit voisivat

käyttää hyödykseen. Keskimäärin jokaisessa laitteessa oli 25 turvallisuuspuutetta. Tutkimuksessa ei eritelty laitteita, mutta niitä oli mm. seuraavista kategorioista: televisiot, web-kamerat, termostaatit, pistorasiat, ovien lukot, hälytysjärjestelmät.

Tutkimuksen laitteiden turvattomuuteen löytyi myös yksi yhteinen tekijä, Linux. Useimmat laitteista toimivat Linux-käyttöjärjestelmän ”riisutun” version pohjalta. Ohjelmistossa on hyvinkin perustavanlaatuisia haavoittuvuuksia, ja laitteiden valmistajilla ei ole halukkuutta tai osaamista paikata niitä. Seitsemän kymmenestä testatusta laitteesta lähetti kaiken tuotetun datan Internetiin täysin suojaamattomana, ja kuusi ei suojannut salasanatietoja. Kaiken lisäksi, yhdeksän kymmenestä laitteesta kerää käyttäjältään henkilökohtaisia tietoja, kuten katuosoitteen, syntymäajan, nimen ja sähköpostiosoitteen. (Sorokanich, haettu 22.11.2014.)

Jo lähitulevaisuudessa on mahdollisuus, että kotisi ”hakkeroidaan”. Kun esimerkiksi ulko-ovet, leivinuunit, lämmitysjärjestelmät ja jääkaapit saavat Internet-yhteyden, on niitä tällöin mahdollista hallita etäältä, esimerkiksi sovelluksella tablet-tietokoneella tai älypuhelimella. Voit esimerkiksi hallita talon lämmitystä, avata lukitun ulko-oven, tai katsoa kotiisi sijoitettuja valvontakameroita etäältä olematta itse lähelläkään kotiasi. Aikaisemmin tänä vuonna, eräs laitteiden turvallisuutta tutkiva taho löysi älyjääkaapin, joka oli hakkeroitu ja valjastettu roskapostia lähetteleväksi ”spam-bot:iksi”. Kyseisen jääkaapin omistaja ei luonnollisesti ollut tapahtuneesta tietoinen. Myös huolestuttava tapaus oli, kun perheen lapsen itkuhälyttimeen oli murtauduttu ja tekijä solvasi lasta sen kautta sanallisesti. (Rosenblatt, haettu 22.11.2014.)

Ryhmä Englantilaisia tietoturvan asiantuntijoita onnistui hakkeroimaan tiensä älykodin Wi-Fi (langaton Internet-yhteys) – verkkoon, käyttämällä hyväksi LED-lamppua nimeltään Lifx. Lampun verkkoprotokollasta löytyi tietoturva-aukko, jota hyväksi käyttämällä ryhmä onnistui saamaan itselleen langattoman verkon käytön valtuudet. He onnistuivat murtamaan suhteellisesti helposti verkon salasanan suojauksen, ja näin ollen pääsivät käyttämään sitä vapaasti. Huolestuttavaa on se, että Lifx – lampuissa käytettävää teknologiaa käytetään laajalti muissakin sovellutuksissa. Ryhmä onnistuikin kehittämään eräänlaisen yleisavaimen, jolla on mahdollista murtautua mihin vain verkkoon, jossa käytetään myös Lifx – lamppuja. (Crist, haettu 22.11.2014.)

Useat IoT-laitteet kärsivät rajoittuneista tietoturvaominaisuuksista niiden vähäisen laskentatehon takia. Esimerkiksi suurin osa laitteista ei tue riittävästi käyttäjien tunnistukseen liittyviä teknologioita, jättäen järjestelmien ylläpitäjille vain huonoja, tai jopa ilman vaihtoehtoja. Tämän takia organisaatioiden voi olla erittäin vaikeaa ottaa Internet of Things osaksi laitteistoaan, kun niille ei voida taata turvallista pääsyä verkkoon. Tätä ongelmaa korostaa entisestään liika innokkuus muiden yrityksen osastojen osalta saada laitteita käytettäväksi, kysymättä IT-osaston mielipidettä. Laitteiden käyttöönotto kun on usein haastavampaa, kuin hankkija ennakkoon olisi voinut kuvitella. (Liu, haettu 22.11.2014.)

Kotikäytössä IoT-laitteet muodostavat keskenään verkottuneita kokonaisuuksia. Käsitteellä hubi tarkoitetaan ”suurempaa” laitetta, johon kaikki muut lopulta yhdistetään. Käyttäjä pystyy itse hallitsemaan hubia, ja siinä on myös itsessään älykkyyttä. Se, mikä usein pääsee valmistajilta ja käyttäjiltä tässä kokonaiskuvassa unohtumaan on, mistä lopulta yleensäkin saadaan kotiin Internet-yhteys. Kyseessä on siis modeemi/reititin. IoT-laitteiden turvallisuus ei siis itsessään vielä ole riittävä, jos jo aikaisemmassa vaiheessa ketjua on turvaton verkkolaite, modeemi/reititin.

Aikaisemmin tänä kuluvana vuonna kävi ilmi, että eräiden suurimpien verkkolaitteiden valmistajien laitteissa oli vakava tietoturva-aukko. Ulkopuolinen asiansa tunteva henkilö pystyi murtautumaan haavoittuvuuden kautta modeemilaitteeseen ja lopulta ottamaan sen vapaasti hallintaansa. Tämä mahdollistui vanhan, laajalti käytetyn SNMP – verkkoprotokollan kautta. Modeemeihin/reitittimiin, joissa kyseinen haavoittuvuus oli, valmistaja julkaisi päivityksen, jolla luvattiin korjata mahdollinen ongelma. Käyttäjä, allekirjoittanut mukaan luettuna, joutui itse ottamaan asiasta median kautta selvää ja tekemään päivityksen. Tämän takia käytössä voi olla vielä suuriakin määriä laitteita, joissa tietoturva-aukko vielä on olemassa.

Verkkolaitteiden valmistajien tulisikin käyttää lähitulevaisuudessa enemmän aikaa kehitystyöhön, taatakseen laitteidensa turvallisuus, etenkin kun IoT arkipäiväistyy kovalla vauhdilla. Tilanteessa tarvittaisiin yhteistyötä eri valmistajien välillä, jotta turvallisuus ja yhteensopivuus saataisiin maksimoitua. Kun valmistajia ei varsinaisesti kiinnosta kuin oman tuotteensa turvallisuus, niin kokonaisuudessa saattaa ilmetä

vielä entistä isompiakin ongelmia tulevaisuudessa. Uuden tuotteen kehitystyössä pitäisikin aina lähteä ensin liikkeelle sen turvallisuuden takaamisesta.

3 IOT-PROTOKOLLAT

3.1 Protokolla käsitteenä

Käsitteellä protokolla tarkoitetaan sääntöjä ja sopimuksia, joiden avulla verkottuneet laitteet keskustelevat toistensa kanssa. Protokollat tietokoneverkoissa käyttävät yleisesti pakettivälitystä/pakettikytkentää hyödyntäviä tekniikoita, kun ne lähettävät sekä vastaanottavat ”viestejä” pakettimuotoisena. Protokollat sisältävät mekanismeja, joilla laitteet voivat tunnistaa ja muodostaa yhteyksiä toistensa välille, kuin myös muotoilutietoa, joka kertoo miten data pakataan lähetettäviin ja vastaanotettaviin viesteihin. Jotkin protokollat tukevat myös viestien tunnistamista ja datan pakkaamista, joita käytetään kommunikaation tilanteissa, jossa vaaditaan luotettavuutta ja/tai korkeaa suorituskykyä. On olemassa satoja erilaisia protokollia, jotka usein ovat suunniteltu tiettyä tarvetta tai ympäristöä varten.

Internet-protokollien ”perhe” sisältää joukon toisiinsa liittyviä, useimmiten käytettyjä protokollia. IP-protokollan (IP) lisäksi on olemassa korkeamman tason protokollia, kuten TCP, UDP, HTTP, FTP, jotka kaikki integroituvat IP:hen, tuoden sille lisäominaisuuksia. Vastaavasti matalamman tason protokollat, kuten ARP ja ICMP, myös toimivat yhdessä IP-protokollan kanssa. Yleisesti ottaen, korkeamman tason IP-protokolla – perheen protokollat ovat enemmänkin tekemisissä sovellusten, esim. Web-selainten kanssa, kun matalamman tason protokollat ovat vuorovaikutuksessa verkkoadapterien ja muun tietokonelaitteiston kanssa. On olemassa myös reititysprotokollia, jotka ovat erityistarpeisiin, esimerkiksi reitittimien käyttöön suunniteltuja, Internetissä käytettyjä protokollia. Tavanomaisia reititysprotokollia ovat EIGRP, OSPF, ja BGP.

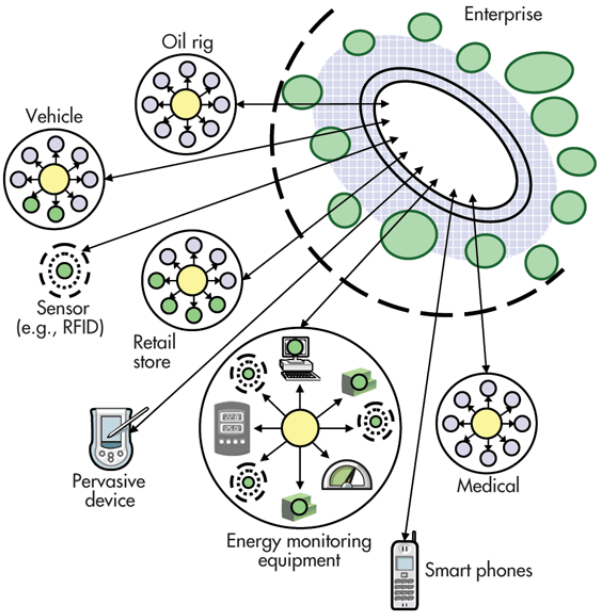
Modernit käyttöjärjestelmät, kuten Microsoftin Windows, sisältävät sisäänrakennettuja palveluja tai taustaprosesseja, jotka tukevat joitain protokollia. Ohjelmat, kuten

Web-selain, sisältävät ohjelmakirjastoja, jotka tukevat korkean tason protokollia, joita ohjelma tarvitsee toimiakseen. Joidenkin matalan tason – protokollien (IP, reititys) tuki luodaan suoraan tietokoneen laitteistoon valmistusvaiheessa, paremman suorituskyvyn toiveissa. Ryhmää protokollia, jotka toimivat yhdessä niin korkealla kuin matalalla tasolla, kutsutaan protokollaperheeksi. Protokollaperhettä mallinnetaan usein OSI – mallilla, jossa protokollat järjestetään käsitteellisiin tasoihin (engl. layers) ymmärryksen helpottamiseksi. (Mitchell, haettu 19.11.2014.)

3.2 MQTT

MQTT (Message Queue Telemetry Transport) on kehitetty keräämään laitteelta tietoa. Nimensä mukaisesti, sen ensisijainen käyttötarkoitus on kaukomittaus, telemetria tai etävalvonta (engl. remote monitoring). Sen tehtävänä on kerätä kaikenlaista dataa laitteilta, jotka ovat jollain tavalla mukana IT – infrastruktuurissa. Sitä voidaan käyttää niin suurissa verkoissa, kuin pienille laitteille, joita tarvitsee seurata tai ohjata, esimerkiksi pilvestä/pilvipalvelusta. MQTT ei yritä mahdollistaa laitteelta laitteelle tapahtuvaa tiedonsiirtoa tai levittää dataa usealle eri vastaanottajalle. Koska sillä on vain yksi selkeä tehtävä, se onkin hyvin yksinkertainen ja tarjoaa vain muutamia ohjausvaihtoehtoja. Sen ei tarvitse myöskään olla erityisen nopea toiminnaltaan. Tässä tapauksessa, termillä ”reaaliaikainen” tarkoitetaankin muutaman sekunnin aikana tapahtuvaa toimintaa.

MQTT toimii luonnostaan hub-and-spoke (suom. säteittäinen kuljetustoiminta) – arkkitehtuurin mukaisesti. Kaikki laitteet yhdistyvät datan keskittävään palvelimeen. Dataa ei haluta menevän hukkaan, joten protokolla toimii TCP:n (tietoliikenneprotokolla) päällä, jolloin tietovirta on yksinkertainen ja luotettava. MQTT mahdollistaa sovellutukset, joissa esimerkiksi valvotaan isoa öljyputkea vuotojen tai vandalismin varalta. Kaikki käytettävät, tuhannet sensorit tulee keskittää yhteen paikkaan analyysia varten. Kun järjestelmä havaitsee ongelman, voi se tehdä tarvittavia toimenpiteitä sen korjaamiseksi. Muita käyttökohteita MQTT – teknologialle ovat esimerkiksi virrankulutuksen monitorointi, valaistuksen hallinta, ja jopa älykäs puutarhanhoito. Niissä kaikissa on tarve kerätä dataa useista eri lähteistä ja mahdollistaa sen jakaminen edelleen IT – järjestelmille. (Schneider, haettu 24.11.2014.)



Kuva 2: MQTT ”hub-and-spoke”

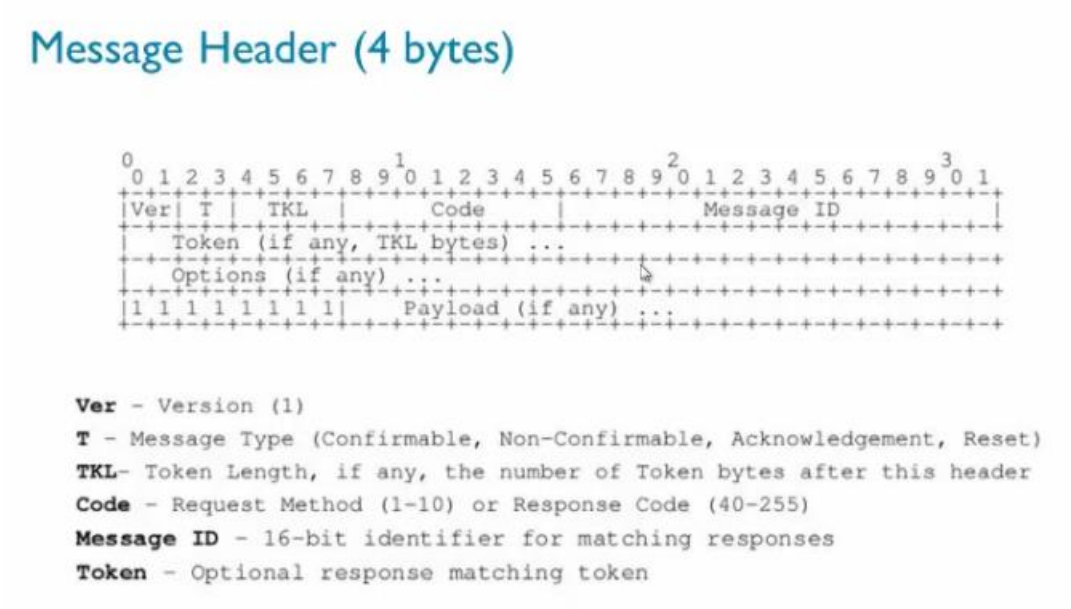
3.3 CoAP

CoAP (Constrained Application Protocol), joka tunnetaan myös lempinimellä the Web of Things Protocol, on avoin IETF – standardi. CoAP on suunniteltu käyttöön, jossa tarvitaan protokollaa rajoitettuun (tiedonsiirtonopeus kilobittejä sekunnissa), suljettuun, tai esimerkiksi vähävirtaisiin ympäristöihin. CoAP tukee yhteiskäyttöä UDP:n, SMS:n, ja TCP:n kanssa. Protokolla sisältää vahvan, sisäänrakennetun tietoturvan, käyttäen hyväksi DTLS:ää (Datagram Transport Layer Security). Protokolla on täysin asynkroninen (Asynchronous Subscription). CoAP on hyvin suorituskykyinen RESTful – protokolla. CoAP tekee käytettävästä verkosta suorituskykyisen ja hyvin yhteensopivan, käyttökelpoisen Internet of Things – sovellutuksille. CoAP suunniteltiin tukemaan mahdollisimman hyvin REST:iä (arkkitehtuurimalli rajapinnoille). Se tukee ”nukkuvia laitteita”. Protokollaa voidaan käyttää erilaisissa yhteyden tilanteissa, kuten peer-to-peer (laitteelta toiselle) tai laitteelta verkon palveluun.

CoAP sisältää mm. seuraavanlaisia ominaisuuksia:

- sulautettu siirto – protokolla (engl. embedded web transfer)
- asynkroninen transaktiomalli
- UDP binding

- Multicast – tuki
- metodit GET, POST, PUT, DELETE
- URI – tuki
- pieni, yksinkertainen neljän bitin header (otsikko/ylätunniste)



Kuva 3: CoAP – protokollan header

(Shelby, haettu 26.11.2014.)

CoAP on erikoisprotokolla Web – ympäristöjen tiedonsiirtoon, joissa solmut ja verkko ovat rajoittuneita, esimerkiksi vähäisen tehon ja hävikin takia. Solmuilla on usein 8 – bittiset mikrokontrollerit, joilla on vähän ROM- ja RAM – muistia. Vastaavasti verkoissa voi olla korkea pakettihävikin aste ja huono suoritusteho (esim. 10 kbps). Protokolla on suunniteltu machine-to-machine – sovellutuksille ja rakennusautomaatioon. CoAP sisältää request/response keskustelumallin, tukee sisäänrakennettuna palveluiden ”löytämistä” (engl. discovery of services), sisältää Webin tärkeimpiä ominaisuuksia, kuten URI:t ja Internet – median tyypit.

CoAP:in keskustelumalli on samantyyppinen, kuin HTTP:n asiakasohjelma/palvelin – mallissa. CoAP:in request on samanlainen HTTP:n vastaavaan, ja sen lähettää asiakasohjelma, joka vaatii toimintoa resurssiin palvelimella. Palvelin tällöin vastaa viestiin Response Code:lla. CoAP määrittelee neljä erityyppistä viestiä: confirmable, non-confirmable, acknowledgement, reset. Loogisesti ajateltuna CoAP voitaisiin

nähdä kaksikerroksisena: viestikerros, joka huolehtii UDP:sta ja luonteeltaan asynkronisista interaktioista, ja request/response kerros, jossa käytetään koodeja Method & Response. CoAP on kuitenkin vain yksittäinen protokolla, jossa viestittely ja request/response ovat vain CoAP – header:in ominaisuuksia. CoAP – keskustelumalli perustuu viestienvaihtoon päätelaitteiden välillä käyttäen UDP:tä. Jokainen viesti sisältää Message ID:n, jolla havaitaan mahdolliset duplikaatit. Message ID on kompakti: sen 16 – bitin koko mahdollistaa kahdensadanviidenkymmenen viestin lähettämisen yhtä sekuntia kohden päätelaitteelta toiselle. CoAP request sisältää metodin, jota käytetään resurssiin, resurssin tunnisteen, tietosisällön, Internet – median tyypin, ja vaihtoehtoisen request:in metadatan.

CoAP – palvelimet yleensä vastaavat request – pakettiin response – paketilla. Response voi olla merkittävästi suurempi, kuin request. Hyökkääjä voi käyttää CoAP – solmuja muuttaakseen pienen hyökkäyspaketin suureksi; tekniikka tunnetaan nimityksellä amplification. On siksi olemassa vaara, että CoAP – solmut voivat yhdistyä Denial of Service (DoS) – hyökkäyksessä, käyttäen hyväksi protokollan voimistavia ominaisuuksia. Hyökkääjä yrittää ylikuormittaa kohteen kasvattamalla dataliikenteen määrää. Hyökkääjä tarvitsee vain kohteen IP – osoitteen ja soveltuvan request – paketin, jolla ohjataan liian suuri paketti uhrille. (Shelby, ym. haettu 26.11.2014.)

3.4 XMPP

XMPP (Extensible Messaging and Presence Protocol) tunnettiin aikaisemmin nimityksellä ”Jabber”. Se kehitettiin pikaviestintään, jossa ihmiset pitävät yhteyttä toisiinsa tekstiviestein. Protokollan nimessä (Presence, läsnäolo) piilee sen perimmäinen käyttötarkoitus; ihmiskontakti liittyy siihen olennaisesti. XMPP käyttää XML - tekstiformaattia alkuperäisenä luokkanaan, joten sille on ominaista ihmistenvälinen kommunikaatio. Samoin kuin MQTT, XMPP toimii TCP:n päällä. IoT:n tapauksessa XMPP tarjoaa helpon tavan ”puhutella” laitteita. Tämä on erityisen hyödyllistä, jos data kulkeutuu pitkälle, läpi toisiinsa liittymättömien pisteiden. XMPP ei ole suunniteltu olemaan nopea. Monet sovellutukset käyttävät ”kiertokyselyä”, tai tarkastuksia päivityksien varalle, vain tarvittaessa. Protokolla tarjoaa hyvän tavan, esimerkiksi kytkeä kotisi termostaatti Web – palvelimeen, jolloin sitä voidaan hallita älypuheli-

mella. Sen vahvuuksiin kuuluu osoittaminen (engl. addressing), tietoturva, ja skaalautuvuus. (Schneider, haettu 24.11.2014.)

3.5 AMQP

AMQP (Advanced Message Queuing Protocol) perustuu jonoihin (engl. queue). Se lähettää transaktioviestejä (haku, tallennus) palvelimien välillä. Viestikeskeisenä, aikaisemmin pankkitoiminnassa käytettynä väliohjelmistona, se voi käsitellä luotettavasti tuhansia, jonotusta vaativia transaktioita. AMQP keskittyy siihen, että viestejä ei mene hukkaan. Luotettavuuden takia, AMQP käyttää TCP:tä. Päätelaitteiden tulee tiedostaa jokaisen viestin hyväksyminen. Syntyperänsä pankkitoiminnassa seurauksena, väliohjelmisto keskittyy jokaisen viestin seuraamiseen. Jokaisen viestin perillemeno varmistetaan, vaikka välillä tapahtuisi häiriöitä tai laitteiden uudelleenkäynnistymisiä. Protokollaa käytetään useimmiten liiketoiminnan viestienvaihdossa. Sen tapauksessa laitteet ovat usein älypuhelimia/laitteita, jotka kommunikoivat tukitoimintojen palvelinkeskusten kanssa. IoT:n tapauksessa AMQP soveltuu parhaiten esimerkiksi palvelinpohjaisten analyysi – toimintojen suorittamiseen. (Schneider, haettu 24.11.2014.)

AMQP jäsentää kommunikaation julkaisuina ”vaihtajalle” (engl. publication to exchange), reitittäen vaihtajien ja jonojen välillä, ja sitten merkiten tiedon jonoihin. Vaihtajat kontrolloivat sitä, mihin viestit menevät. Ne voivat esimerkiksi välittää viestejä yksittäiseen jonoon, levittää viestejä useiden jonojen välillä, toistaa jokaisen viestin useisiin jonoihin, tai toimittaa viestejä tietyn kaavan perusteella. Vaihtajat ja jonot ”asuvat” välittäjän (engl. broker) sisällä. Välittäjän ”voima” on näiden toimitusmallien, reititysten joustavuudessa. Reititys on kotoperäistä AMQP – välittäjille. ”Indirectionin” (ohjelmoinnin käsite) taso antaa toimintamallille joustavuutensa pohjan. Kommunikaatio julkaisijalta vaihtajille, ja jonoista ”tilaajille” (engl. subscriber) käyttää TCP:tä, joka tarjoaa luotettavan pisteeltä pisteelle tapahtuvan yhteyden. (Schneider, haettu 24.11.2014.)

3.6 Z-Wave

Z-Wave on lyhyen kantaman, langaton teknologia, jota usein kuvaillaan ZigBee:n suurimmaksi kilpailijaksi. Z-Wave:ista odotetaan tulevan vanhentuneen kotiautomaatio – protokollan, nimeltä X10, seuraaja ja syrjäyttäjä. Pieni tanskalainen ryhmä nimeltään Zensys aloitti aikanaan Z-Wave teknologian kehittämisen. Z-Wave - liittoumaan voi kuulua kolmella eri tavalla: sijoittajana, ”täysipäiväisenä” jäsenenä, ja yhteistyökumppanina. Sijoittajilla ja jäsenillä on mahdollisuus osallistua teknologian kehitykseen, kun yhteistyökumppaneilla on vain pääsy teknologian spesifikaatioihin. Tällä hetkellä suurista yrityksistä, jotka ovat kehityksessä mukana jäseninä, mainittakoon NEC, NTT Docomo, Verizon, ja Zyxel. Aikaisemmin suuret tekijät nimeltänsä Intel ja Cisco, olivat myös mukana teknologian kehityksessä.

Z-Wave:n protokollapino on vertikaalisesti integroitu ja se toimiikin vain sen oman, patentoidun radioteknologian kanssa. Protokolla ei erikseen määrittele yhteen toimivuutta muiden Internet-protokollien kanssa, joten yhdyskäytävän toteutus on täysin tavarantoimittajan harteilla. Käytännössä, yhdyskäytävän toteutuksen tarvitsee muuntaa Z-Wave:n sovellusprotokolla sopivaan esitysmuotoon, esimerkiksi verkkosivustoksi. Z-Wave tarjoaa vain sovellutuksia kotiympäristöön. Z-Wave on selvästi yksi suurimmista kilpailijoista kodin automaation teknologioiden saralla, vaikkakin varsinainen markkinaosuuksien vertailu on vaikeaa. Joidenkin arvioiden mukaan Z-Wave on vahvemmin edustettuna älykodin laitteissa, kuin kilpailijansa. (Mazhelis, Warma, ym., haettu 19.11.2014.)

Z-Wave kotiautomaatio koostuu kolmesta eri tasosta. Radio-taso, verkkotaso ja sovellustaso toimivat yhdessä luodakseen vakaan ja luotettavan verkon, joka mahdollistaa lukuisten solmujen ja laitteiden yhtäaikaisen, toistensa kanssa kommunikoinnin. Radiotaso määrittelee tavan, jolla signaali kulkeutuu verkon ja fyysisen radiolaitteen välillä. Tähän sisällytetään tieto taajuudesta, koodauksesta, jne. Verkkotaso määrittelee miten dataa vaihdetaan kahden laitteen tai solmun välillä. Tähän sisältyy osoittaminen, verkon organisaatio, reititys, jne. Sovellustaso määrittelee mitkä viestit tulee minkäkin sovelluksen käsitellä, jotta saadaan tehdyksi tarvittavia tehtäviä, kuten valokatkaisimen käyttäminen tai lämmityslaitteen lämpötilan vaihtaminen.

Verkkotaso kontrolloi miten dataa vaihdetaan verkossa laitteiden/solmujen välillä. Siihen itseensä sisältyy kolme eri tasoa: MAC (Media Access Layer), kuljetustaso, ja reititystaso. MAC kontrolloi langattomien laitteiden peruskäyttöä. Nämä toiminnot ovat käyttäjille näkymättömissä. Kuljetustaso pitää huolen viestien kuljetuksesta, varmistaen virheettömän, kahden langattoman solmun välisen kommunikaation. Loppukäyttäjä ei voi itse vaikuttaa tämän tason toimintoihin, mutta sen tulokset ovat nähtävissä. Reititystaso hoitaa verkon kapasiteettia, maksimoidakseen verkon kantaman ja varmistaakseen, että viestit saavuttavat määränpäässä olevan solmun. Tämä taso käyttää ylimääräisiä solmuja, mikäli kohde on lähettävän solmun saavuttamattomissa.

Jotta vältyttäisiin matkan varrella hukkaan menneiltä viesteiltä, Z-Wave:n jokainen lähetetty komento ”kuitataan” vastaanottavasta päästä takaisin lähettäjälle. Tämä ei itsessään takaa viestin oikeanlaisesta kuljetuksesta, mutta lähettäjä saa kuittauksessa tiedon muuttuneesta tilanteesta tai mahdollisesta tapahtuneesta virheestä. Vastaanotettua kuittausta kutsutaan nimityksellä ACK (Acknowledge). Z-Wave – lähetin yrittää lähettää viestiä kolme kertaa, odottaessaan ACK:ta. Kolmen epäonnistuneen yrityksen jälkeen lähetin luovuttaa ja ilmoittaa käyttäjälle tilanteesta. Epäonnistuneiden yritysten määrä on myös hyvä indikaattori verkon langattoman yhteyden laadusta.

Verkko koostuu vähintään kahdesta solmusta. Jotta ne voisivat kommunikoida toistensa kanssa, tulee niillä olla pääsy yhteiseen ”mediaan”, tai niillä tulee olla jotain yhteistä. Useimmissa tapauksissa ”media” on fyysinen kommunikaatioväline, kuten kaapeli. Langattomissa tapauksissa signaali kulkee luonnollisesti ilmassa. Langattomia signaaleja käyttää moni muukin teknologia, jolloin tarvitaan määritelty protokolla, joka erottelee solmut toisistaan verkkojen perusteella, ja jättää huomioimatta signaalit muista lähteistä. Jokaisella verkon solmulla tulee olla myös oma, uniikki identiteettinsä erottautuakseen verkon muista solmuista. Z-Wave:n protokolla määrittelee kaksi erilaista identiteettiä verkon organisaatiolle. Home ID on tavanomainen identiteetti kaikille solmuille, jotka kuuluvat yhteen loogiseen Z-Wave – verkkoon. Sen pituus on 32 bittiä. Node ID on yhden yksittäisen solmun osoite verkon sisällä. Sen pituus on 8 bittiä. Solmut, joilla on eri Home ID, eivät voi kommunikoida toistensa kanssa, mutta niillä voi olla samankaltainen Node ID.

Z-Wave sisältää kahta erityyppistä laitteistoa: kontrollereja (laitteet, jotka kontrolloivat muita Z-Wave laitteita) ja orjia (laitteita, joita kontrolloidaan muilla Z-Wave –laitteilla). Kontrollereihin on tehtaalla ohjelmoitu Home ID, jota käyttäjä ei voi itse vaihtaa. Orjilla ei ole valmiiksi ohjelmoitua Home ID:tä, koska ne saavat sen itselleen liittyessään verkkoon. Ensisijainen kontrolleri sisällyttää muut solmut verkkoon antaen niille jokaiselle oman Home ID:n. Jos solmu hyväksyy tämän, tulee siitä osa verkkoa. Kontrolleri myös antaa jokaiselle verkkoon liittyneelle laitteelle Node ID:n. Tapahtuva prosessi tunnetaan nimityksellä Inclusion (suom. sisällytys). Onnistuneen ”sisällytyksen” jälkeen kaikilla solmuilla on sama Home ID. Ne ovat tällöin yhdistettynä samaan verkkoon. Niillä on myös jokaisella oma uniikki Node ID, joten ne voidaan tunnistaa ja yksilöidä toisistaan, ja ne voivat kommunikoida toistensa kanssa. Kontrolleria, jonka Home ID:stä tuli kaikkien laitteiden Home ID, kutsutaan ensisijaiseksi kontrolleriksi. Kaikista muista mahdollisista kontrollereista tulee täten toissijaisia. Ensisijainen kontrolleri voi lisätä verkkoon uusia laitteita, kun taas toissijainen ei. Kuitenkin, kontrollerit ovat toiminnoiltaan täysin samanlaisia.

Koska eri verkoissa sijaitsevat solmut eivät voi kommunikoida toistensa kanssa eriävän Home ID:nsä takia, ne eivät ”voi elää sovussa” ja eivät edes näe toisiansa. 32-bittinen Home ID mahdollistaa jopa neljän miljardin erilaisen Z-Wave verkon määrittelyn. Jokaisessa verkossa voi olla enimmillään 256 erillistä solmua. Kuitenkin, jotkut solmuista on varattu verkon sisäisille toiminnoille ja omalle kommunikaatiolle, joten Z-Wave verkossa voi olla enimmillään 232 laitetta. Solmuja voidaan poistaa verkosta, jonka toimintoa kutsutaan nimityksellä Exclusion (suom. poissulku). Toiminnon aikana laitteelta poistetaan Home ID & Node ID. Laite resetoidaan, palautetaan oletusasetuksiin (kontrollereilla on oma Home ID ja orjilla ei).

Tyypillisessä langattomassa verkossa keskeisellä kontrollerilla on suora langaton yhteys kaikkiin verkon solmuihin. Tähän vaaditaan suora radiolinkki. Tilanteessa, jossa tapahtuu häiriö, kontrollerilla ei ole olemassa ”varareittiä” solmujen saavuttamiseksi, ja tällöin yhteys katkeaa. Z-Wave tarjoaa tehokkaan mekanismin, jolla päästään tämän rajoituksen ylitse. Solmut voivat sekä toistaa, että ohjata viestejä eteenpäin verkon sisällä muille, jotka eivät ole suorassa, kantaman sisäisessä yhteydessä kontrollerille. Tämä mahdollistaa hyvin joustavien ja vakaiden verkkojen luomisen. Kommu-

nikointi voi saavuttaa kaikki verkon sisäiset solmut, vaikka ne eivät olisi suorassa yhteydessä tai, jos yhteys keskeytyy. Kyseisen reititys – järjestelmän käyttö mahdollistaa jopa signaalin kulun ”kulmien” taakse. Muissa teknologioissa toiminnan takaamiseksi vaaditaan usein suora näköyhteys lähettimeltä jokaiselle vastaanottimille. Z-Wave saa signaalin perille tehden kiertotien esteen ohitse, käyttämällä hyväksi tilanteeseen soveltuvaa, toista solmua. Verkon reititys mukautuu automaattisesti kaikkiin verkossa tapahtuneisiin muutoksiin. Mitä useampia solmuja on verkon sisällä, sitä vakaampi ja joustavampi siitä tulee.

Z-Wave kykenee reitittämään viestejä enimmillään neljä toistavan solmun avulla. Jokainen solmu pystyy selvittämään, mitkä solmut ovat suorassa yhteydessä sen langattomaan signaaliin. Näitä solmuja kutsutaan nimityksellä Neighbour (suom. naapuri). Solmun on mahdollista informoida kontrollerille sen naapureista listauksen muodossa. Tätä tietoa hyödyntäen, on kontrollerin mahdollista koota taulukko, jossa on kaikki mahdolliset kommunikaation reitit verkon sisällä. Käyttäjän on mahdollista saada nähdä kyseinen ”reititystaulu”, ja on olemassa useita ohjelmallisia työkaluja, joilla voidaan optimoida verkon järjestelyitä. Kontrolleri yrittää aina ensiksi lähettää viestinsä suoraan kohteelle. Jos tämä ei ole mahdollista, kontrolleri turvautuu reititystauluun määrittääkseen parhaimman saatavilla olevan reitin. Kontrolleri voi valita enimmillään kolme vaihtoehtoista reittiä, ja yrittää lähettää viestiä tarvittaessa niiden kautta. Vain jos kaikki kolme reititystä epäonnistuvat, raportoi kontrolleri tuolloin virheestä.

Orjat kategorioidaan ”tavallisiksi” tai ”reitittäviksi”. Reitittävä orja sisältää edistyneitä reititysominaisuuksia. Kolmen (kontrolleri, orja, reitittävä orja) erilaisen solmutyypin ero on niiden tieto olemassa olevasta reititystaulusta ja niiden kyvystä lähettää viestejä eteenpäin verkolle. Kontrolleri tietää kaikki naapurinsa, pääsee käsiksi reititystauluun, ja voi kommunikoida (jos reitti löytyy) kaikkien verkon laitteiden kanssa. Orja tuntee kaikki naapurinsa, sillä ei ole mitään tietoa reititystaulusta, ja se voi vastata vain solmulle, joka viestin sille on lähettänyt. Reitittävä orja taasen tietää kaikki naapurinsa, pitää hallussaan osittaista tietoa reititystaulusta, ja voi vastata viestin lähettäneelle solmulle ja pystyy myös lähettämään itse ”pyytämättömiä” (engl. unsolicited) viestejä solmuille, joihin sillä on olemassa oleva reitti. Tavallinen orja voi olla laitteena esimerkiksi paikalleen (useimmiten seinään) kiinnitetyt laitteet, kuten kat-

kaisijat, himmentimet, tai sälekaihtimet. Reitittävä orja voi olla esimerkiksi paristoilla toimiva tai muuten ”mobiili” – laite, kuten sensori, termostaatti tai lämmityslaite.

Tyypillinen Z-Wave – verkko alkaa usein muotoutua pienestä kokonaisuudesta, jota voi aina tarvittaessa laajentaa. Pieni verkko voi koostua esimerkiksi kaukosäätimestä ja muutamista katkaisijoista tai himmentimistä. Kaukosäädin toimii ensisijaisena kontrollerina ja hallitsee/tietää katkaisijat/himmentimet. Inclusion:in (sisällytyksen) aikana laitteet (katkaisijat, jne.) tulisi asentaa lopulliselle paikalleen, jotta varmistutaan, että muodostuva lista naapureista olisi mahdollisimman paikkansa pitävä. Tämänlainen verkon konfigurointi toimii niin kauan, kuin kaukosäädin pystyy saavuttamaan kaikki katkaisijat suorasti, eli ohjattava solmu on kantaman sisällä. Jos solmu ei ole kantaman sisällä, voi käyttäjä kokea viiveitä toiminnassa, koska kaukosäätimen tarvitsee havaita verkon rakenne, ennen kun laiteitta voidaan ohjata. Tapauksessa, jossa laite lisättiin ja jälkeenpäin siirrettiin uuteen paikkaan, tätä laitetta voidaan kontrolloida vain jos se on suorassa yhteydessä kaukosäätimeen. Muuten kommunikaatio epäonnistuu, koska reititystaulun merkintä kyseiselle laitteelle on väärin ja kaukosäädin ei kykene tekemään ”verkon skannausta”.

Kaukosäätimet ovat alttiita vahingoille ja hukkaamiselle. Useasti kaukosäätimille ei ole olemassa minkäänlaista varmuuskopioinnin mahdollisuutta. Mikäli ensisijainen kontrolleri vahingoittuu tai menee hukkaan, tarvitsee koko verkolle ja sen sisään kuuluville laitteille tehdä täydellinen ”uudelleensisällytys” (engl. re-inclusion). Kuitenkin laitteita voidaan lisätä verkkoon vielä asennuksen jälkeenkin, jolloin verkosta tulee vakaampi ja verkon uudelleen organisointia ei tarvita. (Vesternet.)

3.7 ZigBee

ZigBee:n teknologian kehitys alkoi vuonna 1998 Motorolan toimesta. Tuolloin, Motorola tutki teknologisia ratkaisuja pienivirtaisiin verkkoratkaisuihin. Tutkinnan myötä muotoutui lopulta vuonna 2003 julkaistu IEEE 802.15.4 – standardi. ZigBee - allianssi perustettiin vuonna 2002, jolloin alkuperäisinä jäseninä oli Motorola, Philips, Invensys, Honeywell sekä Mitsubishi. Tämän jälkeen, useita yrityksiä on liittynyt allianssiin, ja nykyisin yrityksiä (esim. Philips, Texas Instruments, Schneider Elect-

ric) on promoottoreina (edustajia hallituksessa, täydet äänioikeudet) kolmetoista kappaletta. Lisäksi on 170 osallistuvaa tahoa (Telecom, Huawei, Cisco,), joilla on äänestysoikeudet, ja jotka osallistuvat aktiivisesti ZigBee – protokollan kehitykseen. ”Adoptio-yrityksiä”, joilla on pääsy valmiisiin protokollien spesifikaatioihin, on 230 (ABB, Fujitsu, Motorola).

ZigBee – protokollan alkuperäiset spesifikaatiot olivat alun perin kehitetty kotiautomaatioon, mutta nykyisin niitä on saatavilla myös suurille rakennuksille, jälleenmyyntisovelluksille ja terveydenhuollon sovellutuksiin. Useimmat protokollan spesifikaatioista perustuvat radiostandardiin IEEE 802.15.4, mutta viimeisimmät Smart Energy (ekologisuuteen keskittynyt yritys) - määritykset eivät ole enää niin sidottuja aikaisempaan standardiin fyysisesti, sekä käyttörajoitusten puolesta. Määrittelyissä mainitaan myös Internet – yhdyskäytävän toiminnallisuudet, joita voidaan käyttää muuntamaan ZigBee – paketteja Internetin käytölle sopivilla tavoilla. Lisäksi ZigBee – kehyksiä voidaan siirtää TCP:n ”päällä” käyttäen GRIP:iä (gateway remote interface protocol), ja UDP:n (user datagram protocol, yhteydetön protokolla) päällä käyttäen CAP – protokollaa (compact application protocol).

On vaikeaa arvioida asennettujen ZigBee – laitteiden määrää tai markkinaosuutta. Vaikkakin protokollalla on ollut ongelmansa esimerkiksi IP – protokollan yhteensopivuuden kanssa, on se selvästi yksi edelläkävijöistä IoT:n alalla. ZigBee on yksi harvoista protokollista, joka kykenee mukautumaan erilaisille markkinoiden sektoreille. Kenties yksi syy siihen on, että ZigBee – allianssi pyrkii jatkuvasti kasvattamaan yhteentoimivuutta alkuperäisten Internetin protokollien kanssa, jolloin saadaan lisää joustavuutta perustana olevien teknologioiden käytölle. (Mazhelis, Warma, ym., haettu 20.11.2014.)

ZigBee on vähävirtainen, Wi-Fi:n (langaton Internet-yhteys) jatkotuote. Juuri Wi-Fi:ä ja Bluetooth:ia ei tulisi sekoittaa ZigBee:n kanssa. Molemmat Wi-Fi ja Bluetooth ovat kehitettyjä kommunikaatioon, jossa liikutellaan suuria, rakenteeltaan monimutkaisia tiedostoja, kuten mediatiedostoja ja ohjelmia. ZigBee taasen on suunniteltu pienemmän kokoluokan, esimerkiksi sensoreilta saatavan datan siirtoon ja kommunikointiin. Se, mitä ZigBee tuo omalta osaltaan lisää kilpailutilanteeseen muiden ratkaisujen kanssa, on korkea pyrkimys vähävirtaisiin, energiatehokkaisiin,

hintalaatusuhteeltaan korkeisiin, älykkäisiin laitteisiin. ZigBee on suunniteltu pienen datamäärän, kontrollointijärjestelmien sensoreille, joiden kautta data ei liiku kuin maksimissaan 250 kbps (kilobittiä sekunnissa).

ZigBee – laitteet voivat muodostaa verkkoja erilaisten verkkotopologioiden (tietokoneverkon perusrakenne) tavoin. Sallittuja muodostelmia ovat esimerkiksi Mesh (suora yhteys toisiin), tähti, tai Generic Mesh. Verkkoja voidaan laajentaa pienemmistä verkoista muodostettujen ryhmien/rykelmien kautta. ZigBee - verkossa voi olla kolmea erityyppistä solmua: ZigBee Coordinator (ZBC, koordinaattori), ZigBee Router (ZBR, reititin), ja ZigBee End Device (ZBE, päätelaite). Jokaisella kolmesta solmusta on toisistaan poikkeavia, uniikkeja ominaisuuksia.

Jokaisessa verkossa voi olla yksi koordinaattori (ZBC), joka ensinnäkin luo verkon ja säilöö itsellään kaiken tiedon siitä. Laite olisi käytännön sovellutuksessa esimerkiksi ohjauspaneeli tai kaukosäädin olohuoneessa. Luodun verkon kaikki laitteet kommunikoivat kyseisen koordinaattorin kanssa. Sillä on reititysominaisuuksia ja se toimii ”siltana” muihin verkkoihin, esimerkiksi asunnon eri kerroksissa. Reititin (ZBR) on vaihtoehtoinen komponentti, jota käytetään lisäämään verkon peittoaluetta. Aluetta voitaisiin esimerkiksi lisätä niin, että samoilla ZigBee – laitteilla asunnossa, voitaisiin hallita autotallin valaistusta tai lähistöllä olevan vajan ikkunaluukkuja. Reititin itsessään voi ajaa esimerkiksi ohjelmistoon liitettyä valvontakameraa, joka on jatkuvasti aktiivisessa tilassa. Se voi myös vastata (antaa/poistaa) verkon sisällä jaettavista, laitteille annettavista IP-osoitteista. Päätelaite (ZBE) on optimoitu vähävirtaiseksi ja on kolmesta solmutyypistä rahalliselta arvoltaan edullisin. Päätelaite kommunikoi vain koordinaattorin kanssa, ja on myös piste, johon sensorit sijoitetaan. Mikä vain päätelaite, kuten valaisimet, ilmastoinnin osaset, jne. voivat olla ZigBee - päätelaitteita. Jos laitteen Network ID (TCP/IP – tunnisteosa) on vapaana, tehdään Unicast (täsmälähetys, viestin lähettäminen yhteen kohteeseen). Mikäli tämä ei onnistu, tapahtuu Broadcast (yleislähetys, ennalta määräämätön datavirta). Reitittimen tai koordinaattorin vastaus lähetettyyn kyselyyn on tietosisältö, jossa kerrotaan IEEE - standardin osoite, verkko - osoite, ja kaikki muut mahdolliset verkon osoitteet.

Laitesidokset, jotka ovat loogisia linkkejä päätelaitteiden välillä, voidaan luoda, kuten esimerkiksi lampun ohjelmiston sitominen katkaisijan ohjelmiston kanssa. Radio-

lähetin ja prosessori ovat usein rakennettuina samaan mikrosiruun, jotta valmistuskulut saataisiin pidettyä alhaisina. Esimerkkitilanne, jossa henkilöauto ajaa kiinteistölle, auton sisällä oleva radiolähetin ilmoittaa läsnäolostaan ZigBee:n koordinaattorille reitittimien kautta. Seuraavaksi koordinaattori sitoo autotallin ovensulkijan vastaanottimen auton lähettimeen ja kaikki datapaketit auton lähettimestä reititetään ovensulkijalle, joka voi tuolloin avata ja sulkea autotallin oven ilman henkilön poistumista autosta. Koko edellinen tapahtumasarja voidaan automatisoida niin, että auton saapuessa autotallin oven eteen, se aukeaa ajallaan automaattisesti.

Rakennetussa verkossa dataliikenne ja sen määrä voi olla ajoittaista, katkonaista, tai toistuvaa. Kun dataliikenne on ajoittaista, ohjelmisto päättelee datasiirron nopeuden. Katkonainen data tarvitsee optimaalista virransäästöä ja siksi datasiirto on ”virike” – riippuvaista. Toistuvan dataliikenteen tapauksessa käytetään vakiintuneita aikaikkunoita, esimerkiksi ilmastointilaitteen tapauksessa.

ZigBee perustuu IEEE 802.15.4–2003 – spesifikaatioon, joka luo sille perustan/standardit fyysiselle (engl. Physical)- ja MAC – kerrokselle. Protokollapino saadaan valmiiksi lisäämällä siihen vielä ZigBee:n omat verkko- ja sovelluskerrokset. ZigBee käyttää kolmea taajuutta lähetykseen: 868 MHz, 915 MHz, ja 2,4 GHz. Yksikanavaisella 868 – taajuudella on 20 kbps siirtonopeus. Taajuudella 915 MHz on kymmenen kanavaa ja jokaisen kanavan viereinen taajuus eroaa toisesta kahdella megahertsillä. Taajuuden siirtonopeus on 40 kbps. 2,4 Ghz ISM – radiotaajuudella on kuusitoista kanavaa, jokainen niistä viisi megahertsiä ”leveä”, ja saavutettava siirtonopeus on 250 kbps. Lähetyksen aikana kuluvan virran minimoimiseksi, lähettimet käyttävät Energy Detection:ia (ED) ja Link Quality Indication:ia (LQI, kuinka vahva kommunikaatiolinkki on). Kanavien käyttö- ja niiden arviointi on ZigBee:n fyysisen kerroksen vastuulla.

Kanavienhaku tapahtuu pääasiassa tietoliikenteen siirtotien varausmenetelmä CSMA-CA:n (carrier sense multiple access collision avoidance) kautta. ”Solmulta solmulle” – periaatteella, MAC – kerros pystyy pitämään huolen datan lähetyksestä. Lähetyksen tavasta riippuen, MAC – kerros päättää kumpaa CSMA-CA:n moodista, slotted tai unslotted, käytetään. MAC tekee kanavahaun, jakaa PAN ID:t (personal area network identity), löytää uudet verkon laitteet ja synkronoi ne, sekä pitää huolen

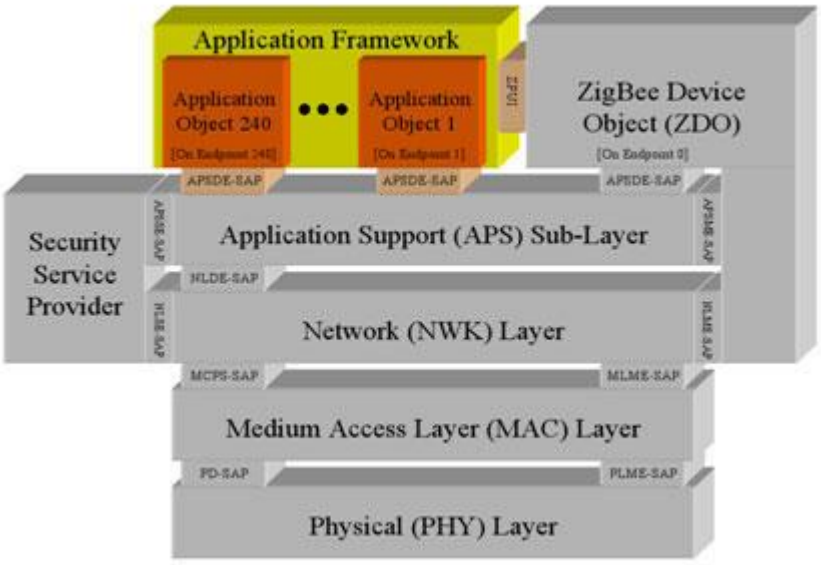
”orvoiksi” jääneistä verkon laitteista. Lisäksi MAC tarjoaa tietoturvaominaisuuksia, kuten pääsyn hallintaa, datan salausta/kryptausta, kaksoiskappaleiden torjumista, sekä kehyksen eheyttämistä (frame integrity).

Verkkokerros pitää huolen verkon käynnistämisestä, laitteiden konfiguraatiosta, verkkotopologiaan perustavasta reitittämisestä, sekä turvallisuuden takaamisesta. Jokaisella solmulla, verkkokerros on se osa pinoa, joka tekee reittien laskemisen, naapurien löytämisen sekä radiovastaanoton. Kaikki solmut ovat optimoituja käyttäen ainutlaatuisia, 64 – bittisiä osoitteita. IEEE 802.15.4 – standardin mukaisesti, tukien maksimissaan 65536 16 – bittistä osoitetta, joilla voi olla 256 aliosoitetta. Verkon reititystaulu luodaan, kun laitteet käynnistetään ensimmäisen kerran generoiden Broadcast Routing Request (RREQ) – paketteja. Päätepisteen (engl. endpoint) reitittimet vastaavat näihin luotuihin paketteihin omilla RREP – paketeilla (routing response packets).

ZigBee:n Application Support (APS) Sub-Layer -kerros on rajapintana verkkokerrokselle sekä sovelluskerrokselle, tarjoten niille joukon palveluita. Palvelut saadaan kahden kokonaisuuden kautta, APSDE (APS data entity) ja APSME (APS management entity), joihin päästään niiden omien SAP:ien (service acces point) kautta. Palveluita ovat esimerkiksi binding management, sovelluskerroksen PDU:iden (protocol data unit) luonti, ryhmien suodatus, ja objekti tietokannan (APS information base) hallinnointi. Edellä mainitut palvelut ovat välttämättömiä sovelluksien virheettömälle toiminnalle.

ZigBee Application Framework, sovellusten viitekehys, on ympäristö, jossa isännöidään sovellusobjekteja (engl. application object), joita käytetään ZigBee – laitteissa. On mahdollista määritellä enimmillään 240 yksilöllistä sovellusobjektia. Viitekehys koostuu sovellusprofiileista, jotka ovat ZDO:n (ZigBee device object) ylin kerros. Sovellusprofiilissa määritellään hyväksytty, datanvaihdon kieli, ja siinä tarjotaan myös yhteentoimivia, eri valmistajien välisiä palveluita. ZigBee – allianssi on julkaissut useita oletusarvoisia sovellusprofiileja, joissa on eriäviä laite – deskriptoreja, joilla on uniikkeja tunnisteita. ZigBee Device Objects (ZDO) tarjoaa rajapinnan sovellusobjektien, laiteprofiilien, sekä ZigBee – laitteiden ASP – kerrokselle. ZDO:t sijaitsevat laiteprofiilien ja Application Support Sub-Layer:in välissä. Ne vastaavat

APS:n, verkkokerroksen ja Security Service Providerin alustuksesta, ja myös muodostavat sovellusten konfiguraatio – tiedon, jotta saadaan toteutettua laitteiden löytäminen, turvallisuus, ja ”network and binding management”.



Kuva 4: ZigBee:n kerroksia

Dataa voidaan siirtää kahdessa eri ”moodissa”: beacon mode, ja non-beacon mode. Beacon mode lähettää dataa verkossa ajoittain. Aikoina, jolloin laitteet eivät lähetä dataa toisilleen, voivat ne siirtyä vähän virtaa kuluttavaan lepotilaan. Verkon reaaliaikaisuus ja synkronisaatio vaativat kuitenkin paljon täsmällisyyttä, kun lähetysajat ovat millisekunteina. Virransäästön ja täsmällisyyden välillä tasapainottelu voikin aiheuttaa verkolle rajoitteita ja nostaa komponenttien hintaa. Non-beacon mode:ssa verkon aktiiviset koordinaattorit ja reitittimet ovat useimmiten ”hereillä” ja odottavat tulevaa dataa, jolloin ne tarvitsevat vakaan virransyötön. Näin ollen päätelaitteet voivat ”nukkua” suurimman osan ajasta ja herätä vain, kun dataa tarvitsee lähettää. Hereillä olevat koordinaattorit/reitittimet ja nukkuvat, ”triggerin” saadessaan heräävät päätelaitteet, muodostavat heterogeenisen verkon, jossa on epäsymmetrinen virranjakelu.

ZigBee, jota jo useat yritykset tukevat maailmanlaajuisesti, on todistanut olevansa hyvä jatke, laajennus jo olemassa oleville standardeille. Se on iso askel kohti laajalti hyväksytyn standardin asemaa. ZigBeen:n huono puoli kuitenkin on se, että verkon

yhden laitteen vikaantuessa, lakkaa koko verkko toimimasta. ZigBee – laitteita käytetään esimerkiksi teollisuudessa, liiketoiminnassa, leluissa, tietokoneen oheislaitteissa, terveydenhuollossa, ja rakennusautomaatiossa. Käytännössä sovellutuksissa vain mielikuvitus on rajana, kunhan kohteessa käytetään langattomia sensori – solmuja ja/tai lyhyen matkan kommunikaatiota. ZigBee on Bluetooth – teknologian mahdollinen kilpailija, ja niiden paremmuus riippuukin vain käyttökohteesta. Lopulta ZigBee voikin olla yhtä aikaa olemassa Bluetooth:in kanssa, aivan kuin tapahtui Bluetoothin ja Wi-Fi:n tapauksessa. (Thakur, haettu 24.11.2014.)

3.8 DDS

DDS (Data Distribution Service) suuntautuu laitteisiin, jotka käyttävät hyödykseen suoraan muilta laitteilta saatavaa dataa. DDS jakaa dataa muille laitteille. Vaikka rajapintoja muuhun IT – infrastruktuuriin tuetaan, sen päätarkoitus on yhdistää laitteita toisiinsa. Se on datakeskeinen väliohjelmisto – standardi, jolla on juuria korkeata suorituskykyä vaativiin sovellutuksiin niin maanpuolustuksessa, teollisuudessa, ja sulautetuissa järjestelmissä. DDS pystyy tehokkaasti välittämään miljoonia viestejä sekunnissa useille vastaanottajille, samanaikaisesti. Laitteet vaativat dataa hyvin eritavalla kuin IT – järjestelmät. Laitteet ovat nopeita. Reaaliaikaisuutta mitataan usein mikrosekunneissa. Laitteiden tulee kommunikoida useiden muiden laitteiden kanssa monimutkaisilla tavoilla, jolloin TCP:n yksinkertaiset, pisteeltä – pisteelle – datavirrat, ovat liian rajoittavia. DDS tarjoaa yksityiskohtaisen QoS (Quality of Service) -palvelun, multicast:in, konfiguroitavaa luotettavuutta, ja kokonaisvaltaista tiedon redundanssia. Hajautettavuus on myös yksi sen vahvuuksista. DDS tarjoaa tehokkaita tapoja suodattaa, ja valita tarkasti mikä data menee mihinkin. Samanaikaisia kohteita voi olla tuhansia. Jotkut laitteet ovat pieniä, jolloin on olemassa ”kevyempiä” (engl. lightweight) DDS – versioita. DDS toteuttaa suoraa laitteelta laitteelle tapahtuvaa väyläkommunikointia.

Tehokkaat, integroidut laitejärjestelmät käyttävät DDS:ää. Se on teknologia, joka tuottaa joustavuuden, luotettavuuden, ja nopeuden, joita tarvitaan monimutkaisten, reaaliaikaisten sovellutusten rakentamisessa. Sovellutuksia on esimerkiksi asevoimi-

en järjestelmissä, tuulipuistoissa, sairaaloissa (esim. kuvauslaitteet), ja seuranta & jäljityslaitteissa. (Schneider, haettu 24.11.2014.)

DDS jäsentää kommunikaation virtuaaliseen, globaaliin datatilaan kahdella tavalla: reads, ja writes. Sitä käyttääkseen tulee määritellä datalle mallit valmiista, tietyn datatyypin aihepiireistä. Sen jälkeen infrastruktuuri kontrolloi, miten dataa käytetään ja miten siihen pääsee käsiksi. Aihepiiri (engl. topic) viittaa tietokannan tauluun ja datan tyyppi ”skeemaan”. Jokainen tyypin kenttä voi olla avain. DDS sallii dynaamiset datamallin vaihdokset, joissa yhdistyy jäsennellyn datan edut ja yksinkertaisen järjestelmän kehittämismahdollisuus. Vaikka DDS mallintaa kaikki kanssakäymiset reads:eina ja writes:eina datatilaan, data virtaa suoraan julkaisijalta/tuottajalta (publisher/producer) tilaajalle/kuluttajalle (subscriber/consumer). Tilanteen välissä ei ole ”broker:ia”. Sen sijaan julkaisija ja tilaaja yhdistyvät toisiinsa ”databus:sin” yli. Hyvin laaja valikoima QoS – parametreja kontrolloi tarkasti miten data virtaa databus:sin lävitse. Väliohjelmisto yhdistää julkaisijan tilaajaan niiden tyypin, aihepiirin ja QoS:n perusteella. Tuloksena on nopea, suora, kontrolloitu kommunikaatioyhteys. (Schneider, haettu 24.11.2014.)

3.9 INSTEON

Insteon mahdollistaa yksinkertaisten, edullisten laitteiden verkottumisen käyttäen voimalinjoja, radiotaajuuksia, tai molempia. Kaikki Insteon – laitteet ovat toistensa vertaisia, joten jokainen laite voi lähettää, vastaanottaa, tai toistaa muiden viestejä ilman, että vaadittaisiin ensisijaista kontrolleria (engl. master controller) tai monimutkaisia, reititys – ohjelmia. Uusien laitteiden lisääminen verkkoon tekee siitä entistä vankemman, kommunikaation uudelleenlähetysten- ja yritysten hoitavan protokollan ansiosta. Voimalinjoilla käytettyinä, Insteon – laitteet ovat yhteensopivia sähkö- ja radioverkoissa siirrettävän protokollan, X10:n kanssa. Kaksikaistainen kommunikaatio voimalinjojen välityksellä ja ilmateitse varmistavat, että viesteille on useita reittejä kulkeutua kohteeseensa.

Insteon – laitteet vastaavat komentoihin ilman havaittavaa viivettä. Sen signaalinopeus on optimoitu kotiautomaatioon. Se on tarpeeksi nopea viiveettömään toimin-

taan, mutta silti luotettava. Komponenttien valmistuskulut ovat pidetty alhaisina. Asennustyö kotona ei vaadi mitään uusia johdotuksia tai kytkentöjä, koska tuotteet kommunikoivat jo olemassa olevien virtajohtojen välityksellä tai ilmateitse. Käyttäjän ei tarvitse itse osallistua verkon pystytykseen, koska kaikilla Insteon – laitteilla on jo valmiiksi yksilöllinen identiteetti (ID) tehtaalta lähtiessään. Laitteet liittyvät automaattisesti verkkoon, kun ne ensimmäisen kerran käynnistetään.

Insteon:in viestit ovat pituudeltaan kiinteitä ja ne synkronoituvat sähköverkon ”nollanylitys – kohdassa” (engl. zero-crossing). Ne eivät sisällä lähteen ja kohteen tiedon lisäksi muita reititystietoja. Insteon on luotettava ja edullinen, koska se on optimoitu käskyttämiseen ja kontrollointiin, ei korkeavauhtiseen dataliikenteeseen. Insteon sallii infrastruktuurin laitteiden, kuten valokatkaisimien tai sensoreiden yhteensä verkottumisen suurissa määrissä, edullisella hinnalla. Insteon toimii itsenäisesti, mutta se voidaan myös ”sillata” muihin verkkoihin, kuten Wi-FI, LAN, Internet, puhelinpalvelut, mediatoistimet. Tämä mahdollistaa sen, että Insteon voi olla osa erittäin hienostuneita, kodin automaation ympäristöjä. (Smarthome Technology, haettu 26.11.2014.)

4 KÄYTÄNNÖN PROJEKTI

4.1 IoT-hanke

Osana opinnäytetyötäni osallistuin koulullani aihepiiriä sivuavaan käytännön projektiin. Projekti alkoi toukokuussa 2014 ja sen kesto oli seitsemän viikkoa. Porin kaupunki myönsi Satakunnan ammattikorkeakoululle rahallisia varoja, jotta saataisiin työllistettyä opiskelijoita kesäksi. Opiskelijoita otettiin joko puhtaasti kesätöihin erilaisiin tehtäviin, tai työt olivat joillekin osa koulutusalaansa kuuluvaa pakollista harjoittelua. Omalta osaltani työ nähtiin kesätyönä, jossa osallistuin projektiin, joka toisi lisäsisältöä varsinaiseen opinnäytetyöhöni.

Varsinaiseen projektiin osallistui itseni lisäksi kaksi henkilöä, toinen opiskelija ja opettaja koulutusalaltamme. Projektiin on osoittanut mielenkiintoa myös muutamia

muita henkilöitä, joille projektimme lopputulos tullaan esittelemään demoluontoisesti joulukuun 2014 aikana. Saimme projektillemme työtilaksi vanhan henkilökunnan taukohuoneen. Tilassa tapahtui varsinainen käytännön asennustyö, ja pidimme siellä myös viikoittaiset tapaamisemme/palaverimme. Palaverissa katsoimme missä projektin suhteen sillä hetkellä mentiin, ja mitä olisi tehtävänä seuraavaksi. Selvitettävät asiat ja tehtävät jakautuivat tilannekohtaisesti, ja henkilöiden erityisosaamisen mukaisesti. Kun itse olen käynyt koulutukseni aikana tietyt kurssit ja opiskellut järjestelmäasiantuntijaksi, ja toinen opiskelija vastaavasti ohjelmoitsijaksi, niin työtehtävät jakautuivat usein melko selkeästi. Opettajamme osallistui myös itse aktiivisesti projektin tekemiseen.

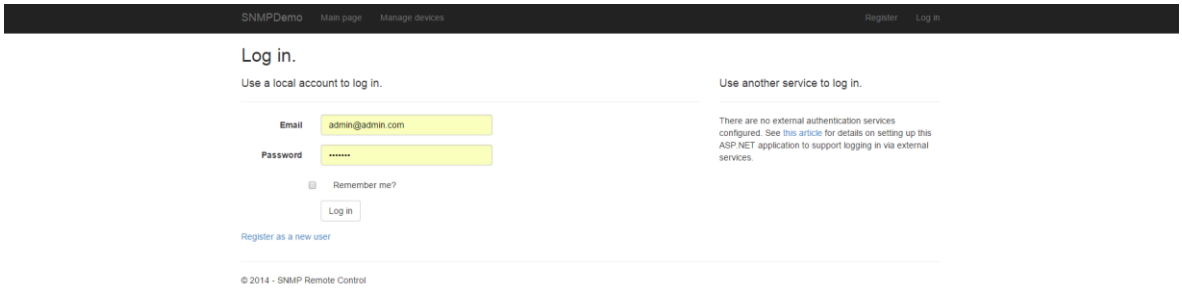
Projektiin osallistuminen oli oman opinnäytetyöni käytännön osuus. Toinen opiskelija, joka teki ohjelmointityön, tekee oman opinnäytetyönsä enimmäkseen sen pohjalta. Hänelle suurin osa opinnäytetyötä on ohjelmoimansa ohjelma, kun minulle se oli Internet of Things ja sen protokollat. Roolini projektissa oli ottaa selvää tarvittavista, projektia tukevista asioista ja antaa tarvittavaa taustatukea, kun oma ohjelmointitaitoni on hyvin rajallinen. Useimmat minulle annetut työtehtävät sisälsivätkin enimmäkseen tiedonhakua Internetistä, ja myöhemmin löytyneen tiedon implementointia projektin asennusympäristöön. Projektin ympäristöön liittyvään laitteeseen (josta myöhemmin lisää) tuli tutustuttua jonkin verran, kun pyrin ymmärtämään sen toimintaa Internetistä ja ohjekirjaan perehtyen. Laitteeseen ja sen käyttöön liittyen, otin selvää muutamista lisäohjelmista, joita sitten pääsimme harjoitteissamme hyödyntämään.

4.2 Älykästä ennakointia

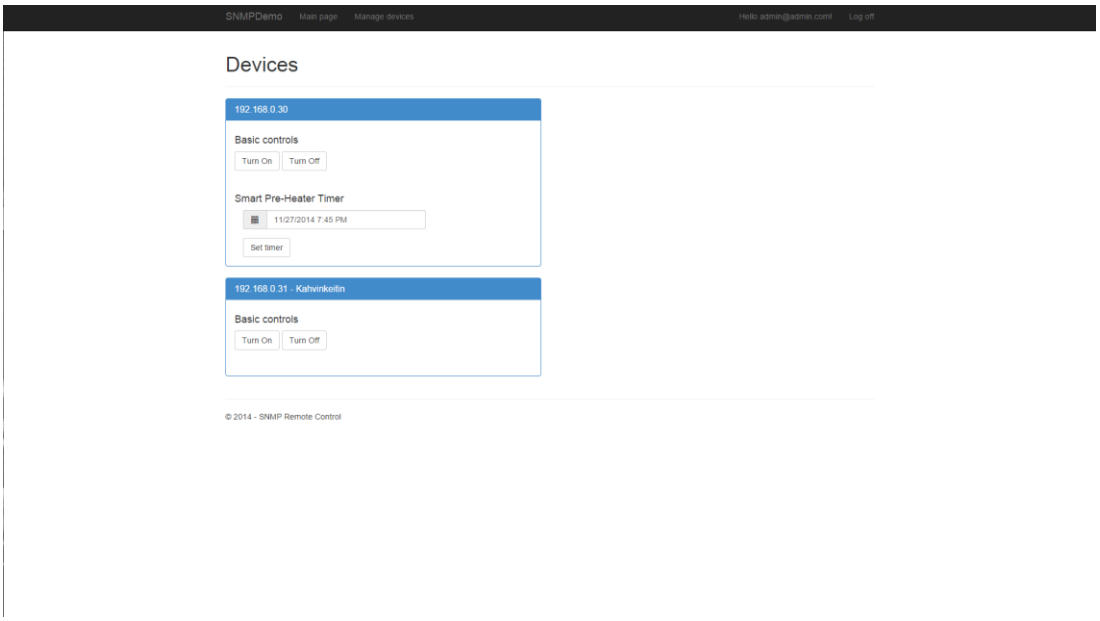
Projektin perimmäisenä ajatuksena oli aikaansaada älykäs, ennakointiin kykenevä ohjelma, joka huolehtii henkilöauton lämmityksestä. Kyseinen ohjelma tarkkailee säätietoja ja päättelee, miten auton lämmitys tulisi hoitaa. Säätiedot saadaan ulkoisesta, Internetin kautta ilmaiseksi saatavilla olevasta säätietopalvelusta. Tämä kyseinen säätietopalvelu käytännön toiminnassa on nähtävissä, kun katselee Internetistä sääennusteita. Palvelun taustalla pyörivät sääennusteet ohjataan ohjelman ”palvelimelle” (projektin tapauksessa tavallinen työasema) ja niitä analysoidaan. Ohjelma päättelee,

laskee saaduista ennusteista sen tiedon, milloin henkilöauton lämmitys tulisi aloittaa. Autoa lämmitetään riittävästi, jotta se olisi henkilön autoa tarvitessaan tiettynä ajanhetkenä valmis. Tarkoituksena on vähentää liiallista lämmityksestä aiheutuvaa sähkönkulutusta. Tietysti myös valmiiksi lämmitetty auto säästää autoa ja luontoa. Ohjelma siis laskee sääpalvelun ennusteista sopivan lämmityksen aloittamisen ajankohdan, ja myös sen lopetuksen.

Käyttäjän näkökulmasta, kaikki taustalla tapahtuva pysyy näkymättömissä. Käyttäjän rooli ohjelman käytössä on yksinkertainen. Käyttäjä syöttää ohjelmaan sen ajankohdan, jolloin henkilöauton halutaan olevan lämmitettynä ja käyttövalmiina. Käyttäjä käyttää ohjelmaa omalta tietokoneeltaan tai älylaitteillaan (puhelimet, tabletit). Ohjelmaa käytetään kirjautumalla tiettyyn osoitteeseen Internet – selainta käyttäen. Ohjelmassa voi olla käyttäjällä kerrallaan useampiakin hallittavia laitteita. Käyttäjä voi myös ajastaa valmiiksi lämmityksiä mielensä mukaan, esimerkiksi tietyt ajastusajankohdat tietyille viikonpäiville.



Kuva 5: Käyttäjän kirjautumissivu

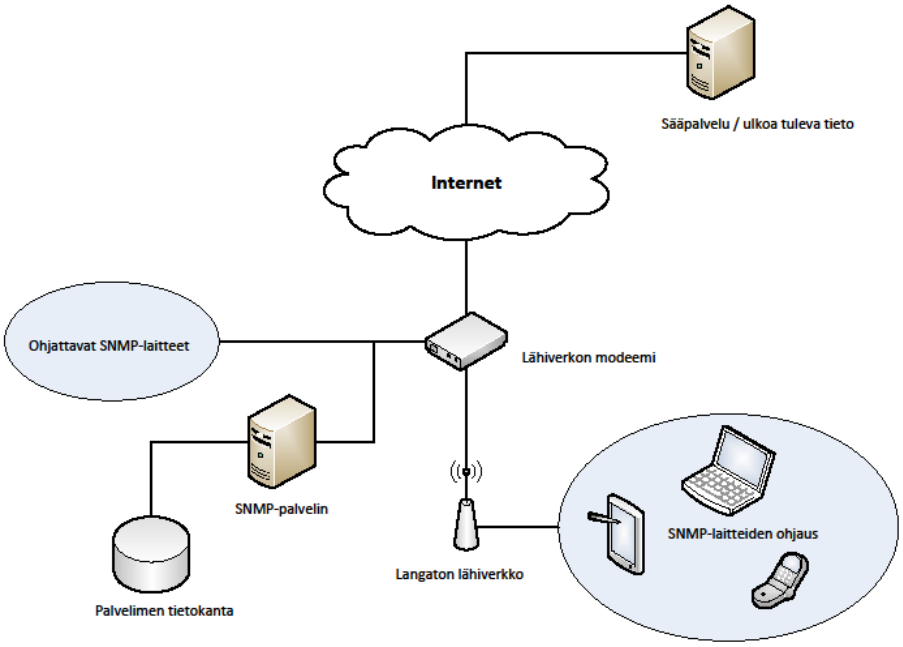


Kuva 6: Laitteiden hallintasivu

Ohjelma ei itsessään liity suoranaisesti ja totutulla tavalla Internet of Things:iin, jossa laitteet tai sensorit keskustelevat keskenään ja ovat älykkäitä. Ohjelman älykkyys ja se, kuinka laiteympäristöstä löytyvä pistorasia on ohjattavissa IP – osoitteilla, ovat IoT:lle ominaisia. Laitteiden välinen Internet – yhteys ja toisten hallinta tulevat yleistymään jatkossa entisestään, jolloin projektin ympäristöstä saadaan kuitenkin näkökulmaa Internet of Things:in maailmaan.

4.3 Projektin laitteisto

Ohjelma ja kaikki siihen liittyvät oheisohjelmistot ja kokonaisuudet (esimerkiksi tietokanta) asennettiin tavalliselle tietokoneelle, työasemalle. Varsinaisen palvelinlaitteen käyttäminen tässä yhteydessä ei ollut tarpeellista. Työaseman, tavallisen modeemin/reitittimen, ja IP – pistorasian yhdistelmällä, oli mahdollista aikaansaada toimiva demoympäristö.



Kuva 7: Laiteympäristön havainnointikuva

Laiteympäristössä modeemilaite on keskeisessä roolissa. Siihen yhdistyvät suoraan ympäristön työasema ja IP – pistorasia. Laite jakaa lisäksi työtilaan WLAN - yhteyttä, johon ympäristön älypuhelin ja tablet ottavat yhteyden. Laiteympäristöstä on myös mahdollista saada yhteys ”ulkoverkkoon”, mutta käytännössä ympäristö on suljettu. Henkilöauton lämmityslaitetta ympäristössä simuloitiin työpöytätuulettimella, sekä pöytälampulla. Näiden avulla seurattiin meneekö ohjelman suorittamat käskyt perille, ja myös ajastusten toimivuus varmistettiin. Nämä laitteet kytkettiin IP - pistorasiaan. Oikeassa realistisessa ympäristössä pistorasiaan kytkettäisiin auton lämmityslaitteisto.

IQsocket IQSW-IP10 mahdollistaa minkä vain siihen kytketyn sähkölaitteen hallinnan. Hallinta tapahtuu IP – verkkojen avulla, kuten esimerkiksi Internet. Pistorasiaa voidaan hallita millä vain laitteella, joka tukee Internet – selainta (HTTP – protokolla), kuten tavallinen tietokone, älypuhelin, jne. Laitetta voidaan myös hallita SNMP (Simple Network Management Protocol) – protokollalla. Juuri laitteen SNMP – ominaisuutta käytettiin hyväksi projektimme ympäristössä.

Laite sisältää seuraavia ominaisuuksia:

- Painonappi laitteen manuaaliseen hallintaan
- ”Watch dog” – toiminto, vahtii pakettihävikkiä
- Ajastusominaisuus, laitteen käynnistäminen tiettynä päivänä tai kellonaikana
- Laitteiden kontrollointi HTTP:llä ja SNMP:llä
- Parametrien konfigurointi, salasanasuojaus
- XML, HTML status – sivu
- Voi lähettää SNMP ”träppejä”
- IQLocator, löydä automaattisesti IQsocket – laitteesi verkon sisällä, IP – osoitteen asetus, laiteohjelmiston päivitys
- Laitteen sisäinen lämpötilasensori
- Event log, kirjaa ylös laitteen 50 viimeisintä tapahtumaa
- C/assembler – koodattu firmware, nopeat käynnistysajat

Kuva 8: IQSW-IP10
(IQtronic, haettu 27.11.2014.)

4.4 Projektin merkitys

Projekti oli itselleni henkilökohtaisella tasolla arvokas kokemus. Reilun seitsemän viikon työskentelyn ja tapaamisten aikana sain hyvää kokemusta projektiluontoisesta työstä. Vaikkakaan projekti ei ollut mahdottoman laaja tai pitkäkestoinen, sai siitä silti hyvää näkökulmaa siihen, miten esimerkiksi tulevaisuudessa työelämässä pro-

jektiluontoisesti voitaisiin työtä tehdä. Tiettyihin aikoihin sovitut ja pidetyt palaverit sitouttivat itseäni pitkästä aikaa johonkin selkeään tehtävään. Itselläni on kuitenkin valitettavasti ”alan töitä” ollut liian vähän, jolloin tämä tuli hyvään aikaan juuri ennen koulutuksesta valmistumista.

Itselleni järjestelmähenkilön ja tukihenkilön erikoistumisen seurauksena, ohjelmointi on jäänyt hyvin paljon taka-alalle. Projekti toi minulle käsitystä siitä, miten yleensäkin ohjelmaa tehdään ja minkälaisista osasista se koostuu. En todennäköisesti osaa itse ohjelmoida nyt yhtään aikaisempaa enempää, mutta olen ainakin saanut nähdä ja seurata mistä ohjelmointi ja tehty ohjelma oikein koostuu. Se jäi päällimmäisenä mieleen, kuinka toimitaan ongelmatilanteen tapauksessa. Tieto tulee pitkälti löytää Internetistä hakukoneiden avulla, ja useasti ratkaisu ongelmaan löytyi keskusteluista, joita toiset ohjelmoitsijat ovat käyneet keskenään. Henkilö, jolla on ongelma, kuvailee tilanteen ja toivoo, että muut asiasta enemmän tietävät pystyisivät auttamaan. Tietysti aiheista löytyy myös valmiita apusivustoja ja käyttöoppaita, mutta juuri ihmiskontakti usein selkiyttää tilannetta parhaiten.

Projektin seurauksena saavutettu ohjelma itsessään on mielestäni melko arvokas. Sillä on hyvin paljon potentiaalia ja kehityskelpoisuutta. Valmiille, markkinoilla myytävälle vastaavalle ohjelmalle olisi varmasti kysyntää. Tietysti ohjelmaa on itse melkoisen vaikea ryhtyä jatkojalostamaan niin pitkälle, että sitä voitaisiin myydä valmiina tuotteena. Tämän seurauksena olisikin hyvä ottaa yhteyttä lämmityslaitteistojen tai vastaavien valmistajiin ja katsoa voisiko sieltä kautta seurata jotakin. Mielenkiintoa varmasti yrityksillä on. Nähtäväksi jää, kuinka paljon muutoksia ohjelmaan tulisi tehdä, jotta se saataisiin myyntiin kaikkien saataville. Yritykset voisivat ostaa vain ohjelman idean, koko ohjelman, tai tehdä yhteistyötä, jotta päästäisiin tavoitteeseen. Yksi mahdollisuus olisi myydä kokonaisuutena ohjelman idea, ohjelmallinen pohja, ja ajatus siitä, että mahdollisesti jatkokehitetään sitä yrityksen kanssa yhteistyössä.

5 LOPETUS

Internet of Things on nykyaika ja tulevaisuus samoissa kansissa. Jo tällä hetkellä laitteiden ja sovellutusten määrä on vaikuttava varsinkin, kun otetaan huomioon kuinka nopeasti kaikki on tapahtunut. Mahdotonta on ajatella, mitä tilanne lainkaan on esimerkiksi viiden vuoden päästä. Todennäköisesti IoT on sellaisissa laitteissa tai kokonaisuuksissa, että monet vain uskaltavat unelmoida tässä vaiheessa. Omasta mielestäni IoT tulee sulautumaan ihmisten laitteisiin ja elämiin niin perusteellisesti, että jossain vaiheessa koko käsite Internet of Things unohtuu. Kun nykyisin kummastellaan henkilöä, jolla ei ole vielä älypuhelinta, niin vaikka juuri viiden vuoden päästä ihmetellään henkilöä, jolla ei ole älykelloa ranteessa.

Samalla aikaa, kun moni asia Internet of Things:issä on hyvin, vielä useampi on huonosti. Laitekanta on aivan sirpaleinen, käytetyt teknologiat ovat useimmat toisistaan poikkeavia, puhumattakaan sovellutuksissa käytetyistä protokollista. Opinnäytetyötä tehdessäni törmäsin useisiin kymmeniin eri protokolliin. Protokolliin, jotka usein oli tehty ajamaan samaa asiaa. Tämänlainen kehitys on mielestäni aivan turhaa ja aikaa vievää. Vielä enemmän tulisi tehdä yhteistyötä ja pyrkiä siihen, että saataisiin oikeasti muutama hyvä, eri tarkoituksiin tehty protokolla. Nykyinen hajonta ja kaikki vastaan kaikkia kilpailutilanne liiketaloudellisten voittojen toivossa, on kaikkea muuta, kuin hyvä lähtötilanne. Nykyisin esimerkiksi älykotia suunnitellessa tuleekin ostaa kaikki laitteisto samalta valmistajalta tai tuoteperheestä. Muutoin laitteet eivät toimi keskenään. Usein suurimpien valmistajien tuotteissa käytetty teknologia on vielä kaiken lisäksi patentoitua, joten muiden on aivan turha edes yrittää tehdä yhteensopivia laitteita.

Aloitin opinnäytetyöni teon toukokuussa 2014 lähteiden etsinnällä. Seurasin uutisia ja artikkeleita tiiviisti, lukien niitä vähintään muutamana päivänä viikossa. Nyt marraskuun 2014 lopulla minulla on melko hyvä käsitys siitä, mikä on the Internet of Things. Olen täysin varma siitä, että tämä tietämys tulee olemaan arvokasta tulevaisuudessani, kenties jo lähivuosien aikana.

LÄHTEET

Bartleson, K.The Internet Of Things Is A Standards Thing. Viitattu 22.11.2014. Saatavissa: http://electronicdesign.com/communications/internet-things-standards-thing

Butler, B. Big data and the cloud are becoming mainstream, market watcher says. Viitattu 22.11.2014. Saatavissa: http://www.networkworld.com/article/2464007/cloud-computing/gartner-internet-of-things-has-reached-hype-peak.html

Crist, R. Hackers find security weaknesses with the Lifx smart LED. Viitattu 22.11.2014. Saatavissa: http://www.cnet.com/news/hackers-discover-security-weaknesses-within-the-lifx-smart-led/

Evans, D. Answering the Two Most-Asked Questions About the Internet of Everything #IoE. Viitattu 22.11.2014. Saatavissa: http://blogs.cisco.com/ioe/answering-the-two-most-asked-questions-about-the-internet-of-everything/

Fahrion, M. Data Mashups Will Make The Internet Of Things Useful. Viitattu 22.11.2014. Saatavissa: http://electronicdesign.com/communications/data-mashups-will-make-internet-things-useful

Fahrion, M. Looking Forwards And Backwards On The Internet Of Things. Viitattu 22.11.2014. Saatavissa: http://electronicdesign.com/communications/looking-forwards-and-backwards-internet-things

GlowCap. Viitattu 22.11.2014. Saatavissa: http://www.glowcaps.com/product/

IQtronic. IQSW-IP10. Viitattu 27.11.2014. Saatavissa: http://www.iqtronic.com/products/iqsocket/iqsw-ip10-detail

Kuva 1: The Quantified Self. Viitattu 26.11.2014. Saatavissa: https://www.youtube.com/watch?v=AjBoFhMVpn0

Kuva 2: MQTT ”hub-and-spoke”. Viitattu 26.11.2014. Saatavissa: http://electronicdesign.com/embedded/understanding-protocols-behind-internet-things

Kuva 3: CoAP – protokollan header. Viitattu 26.11.2014. Saatavissa: https://www.youtube.com/watch?v=UxcNNuwJHUo

Kuva 4: ZigBee:n kerroksia. Viitattu 26.11.2014. Saatavissa: http://www.engineersgarage.com/articles/what-is-zigbee-technology?page=3

Kuva 5: Käyttäjän kirjautumissivu. © Niko Sillvan.

Kuva 6: Laitteiden hallintasivu. © Niko Sillvan.

Kuva 7: Laiteympäristön havainnointikuva. © Niko Sillvan & Topi Hellsten.

Kuva 8: IQSW-IP10. Viitattu 27.11.2014. Saatavissa: http://www.iqtronic.com/products/iqsocket/iqsw-ip10-detail

Liu, C. Securing networks in the Internet of Things era. Viitattu 22.11.2014. Saatavissa: http://www.net-security.org/article.php?id=2105&p=2

Mazhelis, O. Warma, H. Leminen, S. Ahokangas, A. Pussinen, P. Rajahonka, M. Siuruainen, R. Okkonen, H. Shveykovskiy, A. Myllykoski, J. Internet-of-Things Market, Value Networks, and Business Models: State of the Art Report. Viitattu 18.11.2014. Saatavissa: http://internetofthings.fi/

Mitchell, B. protocol (network). Viitattu 19.11.2014. Saatavissa: http://compnetworking.about.com/od/networkprotocols/g/protocols.htm

Rosenblatt, S. Lock your doors: Protecting your Internet-connected home. Viitattu 22.11.2014. Saatavissa: http://www.cnet.com/news/lock-doors/

Santori, M. Designing the Industrial Internet of Things. Viitattu 22.11.2014. Saatavissa: http://electronicdesign.com/industrial/designing-industrial-internet-things

Schneider, S. Understanding The Protocols Behind The Internet Of Things. Viitattu 24.11.2014. Saatavissa: http://electronicdesign.com/embedded/understanding-protocols-behind-internet-things

Schneider, S. What's The Difference Between DDS And AMQP? Viitattu 24.11.2014. Saatavissa: http://electronicdesign.com/embedded/what-s-difference-between-dds-and-amqp

Shelby, Z. Constrained Application Protocol (CoAP) Tutorial. Viitattu 26.11.2014. Saatavissa: https://www.youtube.com/watch?v=UxcNNuwJHUo

Shelby, ym. The Constrained Application Protocol (CoAP) RFC 7252. Viitattu 26.11.2014. Saatavissa: https://datatracker.ietf.org/doc/rfc7252/?include_text=1

Smarthome Technology. Insteon Developer's Guide. Viitattu 26.11.2014. Saatavissa: http://rs.cs.iastate.edu/smarthome/documents/Manuals%20and%20Tutorials/Insteon/INSTEON_Developers_Guide_20051014a.pdf

Sorokanich, R. Internet-Connected Appliances Are a Hacker's Dream Come True. Viitattu 22.11.2014. Saatavissa: http://gizmodo.com/internet-of-things-devices-are-a-hackers-dream-come-t-1615038906

Stateham, B. The Internet of Everything. Viitattu 22.11.2014. Saatavissa:

https://www.youtube.com/watch?v=AjBoFhMVpn0

TechCrunch. Internet Of Things. Viitattu 22.11.2014. Saatavissa: http://techcrunch.com/topic/subject/internet-of-things/

Thakur, A. ZigBee Technology. Viitattu 24.11.2014. Saatavissa: http://www.engineersgarage.com/articles/what-is-zigbee-technology?page=1

Tillman, K. How Many Internet Connections are in the World? Right. Now. Viitattu 22.11.2014. Saatavissa: http://blogs.cisco.com/news/cisco-connections-counter/

Vesternet. Understanding Z-Wave Networks, Nodes & Devices. Viitattu 22.11.2014. Saatavissa: http://www.vesternet.com/resources/technology-indepth/understanding-z-wave-networks

Vodafone. What is M2M. Viitattu 22.11.2014. Saatavissa:

http://m2m.vodafone.com/cs/m2m/discover-m2m/what-is-m2m